GeoVision inc
The Vision of Security

GV-ASManager

User's Manual V3.0

ASMV30-A-EN

© 2011 GeoVision, Inc. All rights reserved.
Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and GV series products are trademarks of GeoVision, Inc. *Windows* and *Windows XP* are registered trademarks of Microsoft Corporation.

September 2011

Contents

Note for the User of Upgrading GV-ASManager v
Chapter 1 Introduction 1
1.1 Main Features 2
1.2 Concepts 4
Chapter 2 Installation 6
2.1 System Requirements 6
2.2 Installing the GV-ASManager 7
2.3 Logging in 8
Chapter 3 The Main Screen of GV-ASManager 10
3.1 Main Screen 10
3.1.1 Toolbar 11
3.2 Device View 13
3.2.1 Controls on the Window 13
3.3 Monitoring Windows 16
3.3.1 Controls on the Window 16
3.3.2 Customizing a Monitoring Window 17
3.3.3 Arranging Monitoring Windows 18
Chapter 4 Settings 19
4.1 Setup Flowchart 19
4.2 Adding Controllers 20
4.2.1 Step 1: Configuring a Controller 20
4.2.2 Step 2: Configuring a Door 22
4.3 Setting Cards 25
4.3.1 Adding a Single Card 25
4.3.2 Adding a Group of Cards 28
4.3.3 Importing/Exporting Card Data 28
4.4 Setting Weekly Schedules 30
4.4.1 Step 1: Setting Time Zones 30
4.4.2 Step 2: Setting Weekly Schedules 32
4.4.3 Step 3: Setting Holidays 34
4.5 Setting Access Groups 35
4.6 Setting Cardholders 37
4.6.1 Adding a Cardholder 37
4.6.2 Assigning a Card to a Cardholder 38
4.6.3 Sending SMS Alerts 38
4.6.4 Customizing a Data Field 38
4.6.5 Importing/Exporting Cardholder Data 39

Chapter 5 Video Integration 40
5.1 Mapping Cameras 40
5.2 Accessing a Live View 42
5.2.1 Live Video Window 43
5.3 Accessing a Video Image 44
5.4 The MultiView Window 44
5.4.1 Adding a Matrix View 46
5.5 Retrieving Recorded Video 47
Chapter 6 Anti-Passback 49
6.1 Anti-Passback 50
6.2 Local Anti-Passback 51
6.3 Global Anti-Passback 53
6.3.1 Step 1: Enabling Global Anti-Passback 53
6.3.2 Step 2: Configuring Areas 54
6.3.3 Step 3: Configuring Readers 54
6.3.4 Step 4: Configuring Door Contacts 55
6.3.5 Step 5: Locating Card Holders 56
Chapter 7 Other Functions 57
7.1 System User Setup 57
7.1.1 Adding a New User 57
7.1.2 Editing an Exiting User 59
7.2 Notification Setup 60
7.2.1 Setting SMS Server 60
7.2.2 Setting E-Mail Server 61
7.2.3 Setting Notification 62
7.3 Startup and Backup Setup 64
7.4 Enrolling Fingerprints 65
7.4.1 Connecting to GV-GF Fingerprint Readers 65
7.4.2 Enrolling Fingerprints 66
7.4.3 Uploading Fingerprints to Controllers 67
7.4.4 Uploading Fingerprints to Controllers Using Door Groups 69
7.5 Scanning Driver's Licenses and Business Card 70
Chapter 8 GV-ASRemote 72
8.1 Installing GV-ASRemote 72
8.2 The GV-ASRemote Window 72
8.2.1 Toolbar 74
8.3 Connecting to GV-ASManager 75
Chapter 9 GV-ASWeb 77
9.1 Connecting to GV-ASManager 77

9.2 Accessing Logs 79
9.2.1 Setting Search Criteria 79
9.2.2 Log Window Icons 81
9.2.3 Exporting Logs 81
9.2.4 Defining Columns 81
9.3 Adding and Deleting Controllers 83
9.4 Adding and Deleting Cards and Cardholders 84
9.5 Searching, Adding and Deleting IP Cameras 86
9.6 Setting Schedule 88
9.6.1 Setting Daily Schedule 88
9.6.2 Setting Weekly Schedule 89
9.6.3 Specifying Holiday 90
9.7 Setting Access Groups 90
9.8 Configuring Areas for Anti-Passback 91
9.9 Creating Accounts to Manage GV-ASWeb 92
Chapter 10 GV-TAWeb for Workforce Schedule and Payoff 93
10.1 Connecting to GV-ASManager 93
10.2 Setting Up Workforce Schedule 96
10.2.1 TA Shift: Setting Up a Daily Schedule 96
10.2.2 TA Template: Setting Up a Schedule Template 98
10.2.3 TA Holidays: Setting Certain Dates as Holidays 99
10.2.4 TA Schedule: Assigning Schedules to Employees 100
10.3 TA User: Specifying Hourly Pay 104
10.4 TA Report: Looking Up Records 105
10.5 Creating Accounts to Manage GV-TAWeb 109
Chapter 11 GV-VMWeb for Visitor Management 110
11.1 Connecting to GV-ASManager 110
11.2 Creating Accounts to Manage GV-VMWeb 112
11.3 Creating Visitor Profile 114
11.4 Granting Visitor Access 115
11.5 Searching GV-VMWeb Database 117
11.6 Visitor Self Registration 117
11.6.1 Setting Up Mail Server in GV-VMWeb 118
11.6.2 Creating a Visitor Account 120
11.6.3 Creating a Visit Request 121
Chapter 12 Database Settings 123
12.1 Starting the Database Tools 123
12.2 Creating a Database 124
12.3 Other Database Settings 125

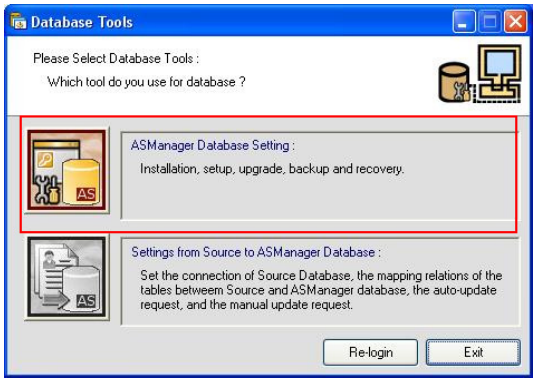
12.4 Source Database Connection....126
12.4.1 Converting Data from the Active Directory Database....127
12.4.2 Converting Data from the OLE Database....128
Chapter 13 Net Module Utility 133
Chapter 14 Troubleshooting 134
Appendix 139
A. Compatible IP Devices....139
B. Event Notifications 140
C. E-Mail and SMS Alert Symbols....144
D. Controller Status 145

Note for the User of Upgrading GV-ASManager

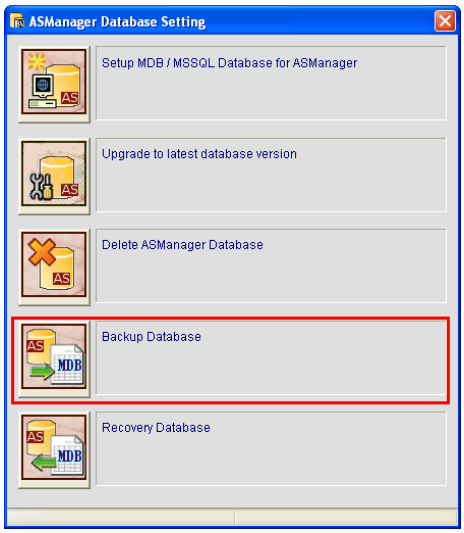
You can keep your current database and upgrade it to work with GV-ASManager version 3.0. Follow the steps below to back up the database of version 2.3 and restore it to the GV-ASManager of version 3.0.

Backing up the Database of Version 2.3

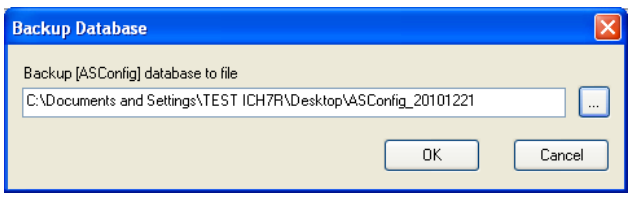
1. Run **ASDBManager.exe** from the V2.3 program folder at **:\Access Control\ASManager**.
2. Select **ASManager Database Setting**.


Database Tools
Please Select Database Tools :
Which tool do you use for database ?
ASManager Database Setting :
Installation, setup, upgrade, backup and recovery.
Settings from Source to ASManager Database :
Set the connection of Source Database, the mapping relations of the tables betweem Source and ASManager database, the auto-update request, and the manual update request.
Re-login
Exit

3. Select **Backup Database**.



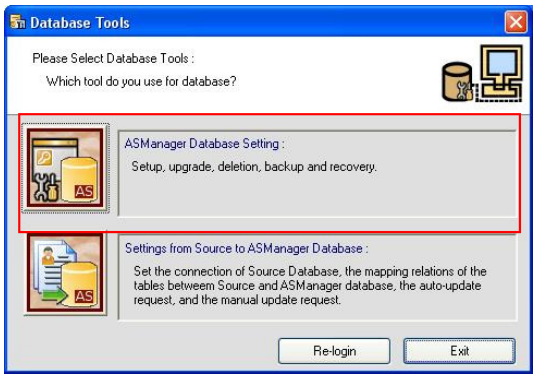
4. Specify a location to save the backup file, and click **OK**.



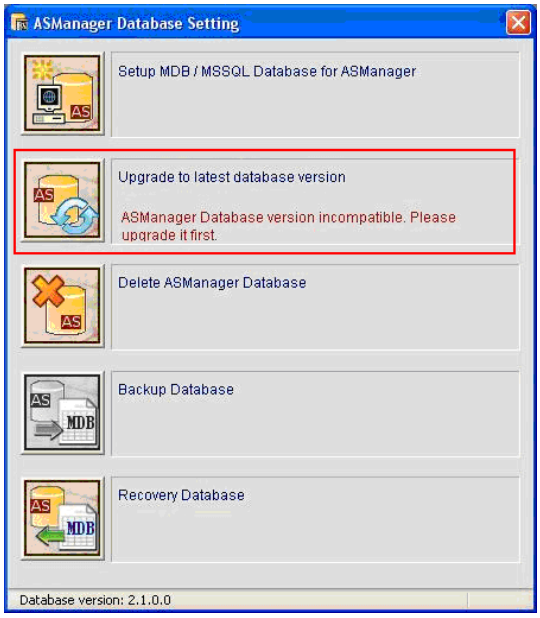
5. When the backup is complete and the message “Backup database successfully” appears, click **OK** and close all open dialog boxes.

Installing GV-ASManager V3.0 and Restoring the Database V2.3

1. Uninstall **GV-ASManager V2.3** before installing the new version.
2. Install **GV-ASManager V3.0**.
3. Run **ASDBManager.exe** from the V3.0 program folder at **:\Access Control\ASManager**.
4. Select **ASManager Database Setting**.

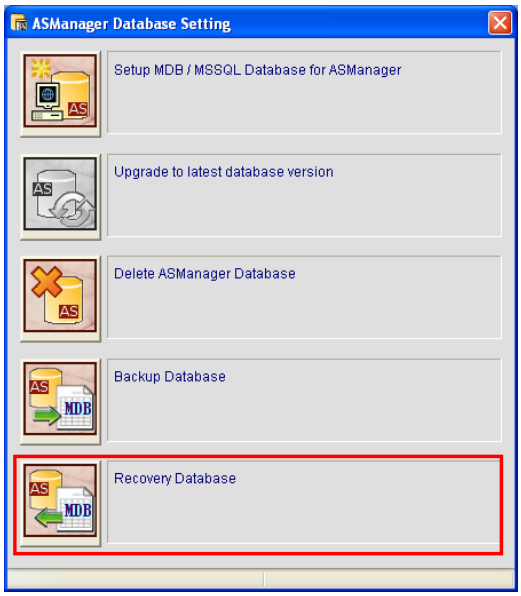

Database Tools
Please Select Database Tools :
Which tool do you use for database?
ASManager Database Setting :
Setup, upgrade, deletion, backup and recovery.
Settings from Source to ASManager Database :
Set the connection of Source Database, the mapping relations of the tables betweem Source and ASManager database, the auto-update request, and the manual update request.
Re-login
Exit

5. Select **Upgrade to latest database version**.

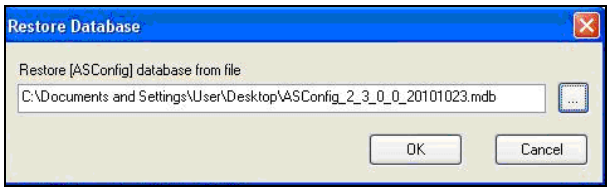

ASManager Database Setting
Setup MDB / MSSQL Database for ASManager
Upgrade to latest database version
ASManager Database version incompatible. Please upgrade it first.
Delete ASManager Database
Backup Database
Recovery Database
Database version: 2.1.0.0

6. The GV-ASManager starts upgrading the database. When the upgrade is complete and the message “Upgrade database successfully” appears, click **OK**.

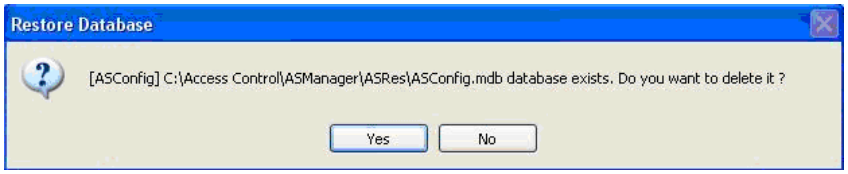
7. To restore the database of version 2.3, select **Recovery Database**.



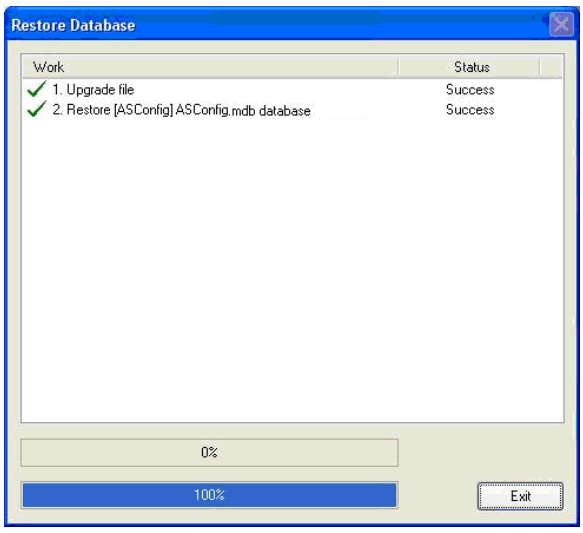
8. Specify the location of the backup database, and click **OK**.



9. When a warning message of the existence of the V3.0 database appears, select **Yes**.


Restore Database
[ASConfig] C:\Access Control\ASManager\ASRes\ASConfig.mdb database exists. Do you want to delete it ?
Yes
No

10. The GV-ASManager starts to restore the database of version 2.3 and convert it to version 3.0.



Chapter 1 Introduction

The GV-ASManager and GV-AS Controller are the combination that offers the full control of the entrances of your premise. Up to 255 units of GV-AS Controllers can be monitored and controlled by one GV-ASManager.

The following diagram is an example of how the GV-ASManager and GV-AS Controller can be set up.

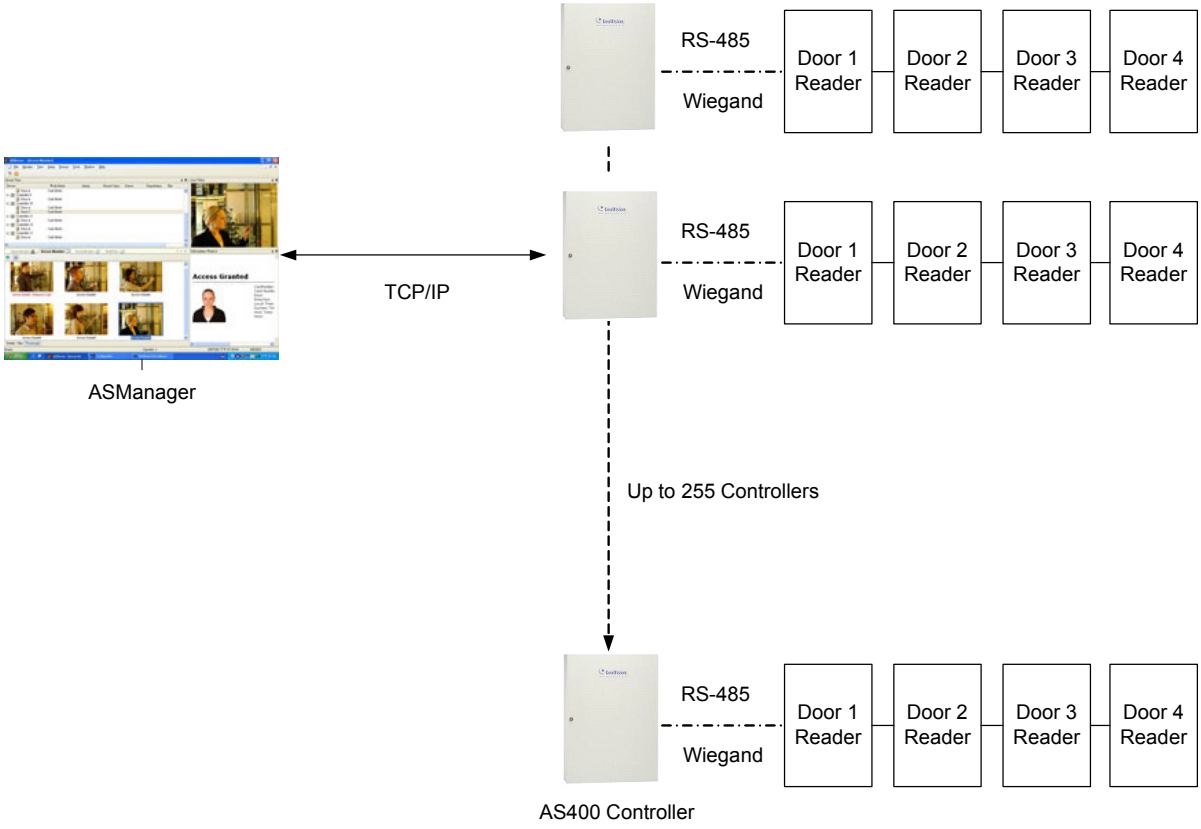


Figure 1-1

1.1 Main Features

GV-ASManager

- Control up to 255 GV-AS Controllers
- Up to 256 time zones and weekly schedules
- Up to 40,000 cards
- Up to 1,000 system users
- Holiday planning for 14 months
- Multiple cards per user
- Four (4) access mode options: Card only mode (default), Card and PIN Code mode, Card or Common mode, Release mode
- Enroll cards in batch mode
- Door alarms: door held open, door forced entry, tamper, access denied
- Duress operation
- Anti-Passback capabilities
- Man trap in double door configuration
- Import/export of card and cardholder data in Access or Excel file format
- User-defined matrix of 16-channel multi-views
- User-defined screen layout and dual monitor display support
- SMS or E-Mail notification with user-defined content, video snapshot and cardholder photo
- Video integration with GeoVision IP devices (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR, GV-IP Camera) and third-party IP cameras
- Support for connecting to third-party IP devices using ONVIF, PSIA and RTSP protocols
- Support Microsoft Access or SQL database

GV-ASRemote

- Monitor unlimited GV-ASManagers over the Internet
- Remote door monitoring, video playback, door operation

GV-TAWeb

- Flexible workforce schedule arrangement
- Payroll calculation
- Attendance and payroll report search

GV-ASWeb

- Remotely add or delete cards, cardholders, controllers, access groups, cameras
- Web interface for historical log search with corresponding video and snapshot
- Log export in Excel, Text, HTML file formats

GV-VMWeb

- Web interface for creating visitor database and granting access
- Visitor record search
- Visitor self registration

1.2 Concepts

Understanding the following concepts may help you read through the manual.

Weekly Schedule	A weekly schedule is certain days of the week when a user is granted access to a secure site. For details, see *4.4 Setting Weekly Schedule.*
Access Group	An access group is a group of cardholders with identical location restrictions during the same time restraints. For details, see *4.5 Setting Access Group.*
Alarm Condition	An alarm condition is a monitored condition through sensing devices, and an alarm condition may activate alarms. For example, the AS100 Controller has the ability to monitor 3 sensors, such as door status sensor, smoke detector and tamper detector. The AS100 Controller also provides 3 output relays for activating and deactivating electric lock, siren and emergency door release when the alarm condition occurs. For settings of alarm conditions see *4.2.2 Step 2: Configuring a Door*. For configuring inputs and outputs see *GV-AS Controller Hardware Installation Guide.*
Anti-Duress	If a person is forced to open the door under threat, he or she can enter his or her PIN plus 1 to activate an alarm and send a signal to the ASManager to dispatch the police. For example, the PIN is 5555 and you enter 5556. The door will open normally (access granted) and the alarm will be activated. The function is enabled by default in the system.
Anti-Passback	The feature is designed to prevent card sharing and to enforce use of entry and exit readers. If a card was used at an entry reader, it must be used at an exit reader before it will be valid at an entry reader again. For settings, see *4.2.2 Step 2: Configuring a Door*.
Interlock	The feature is also called “mantrap” or interlocking”. The feature interlocks two controlled doors allowing only one door to be opened at a time. The feature will not unlock a door if the other door is open. If both doors are open at the same time, the alarm will be activated. For settings, see *4.2.1 Step 1: Configuring a Controller*.

Two-person A/B rule	The door unlock only when two assigned cards are presented together. Two Person Card A must be presented before Two Person Card B. For settings, see *4.3.1 Adding a Single Card*.
IP device	The video device is connected to the ASManager through the network. The ASManager enables you to access the live video from not only GeoVision IP devices (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR and GV-IP Camera) but also certain third-party IP cameras. Connections to IP devices through ONVIF, PSIA and RTSP protocols are also supported. For details, see *Chapter 5 Video Integration*.
Data Group	This feature allows the administrator to restrict a user account to only be able to read, write or execute the controllers, cards, cardholders, access groups, time zones and weekly schedules assigned under a data group. For example, the administrator can create a data group for the sales department and assign sales department-related cards and controllers under that data group. Employees in the sales department will only have access to the cards and controllers of their own department. For details, see *7.1.1 Adding a New User*.
Door Group	When a large number of GV-AS Controllers are connected to the GV-ASManager, the controllers can be organized into different door groups, allowing you to quickly upload fingerprints to all the controllers in a door group instead of uploading to each controller one by one. For details, see *7.4.4 Uploading Fingerprints to Controllers Using Door Groups*.

Chapter 2 Installation

2.1 System Requirements

1. For GV-ASManager version 2.0 or later, the minimum hardware and software requirements are:

OS	32-bit	Windows XP / Vista / 7 / Server 2008
	64-bit	Windows Vista / 7 / Server 2008
CPU		Pentium 4, 3.0 GHz with Hyper-Threading
Memory		2 x 256 MB Dual Channels
Hard Disk		2.0 GB
VGA		NVIDIA GeForce 7300 GT 128MB (PCI slot), or ATI Radeon 9550 / 9600 / X1050 Series 256MB (AGP slot) No support for onboard VGA
DirectX		End-User Runtimes (November 2008)
Software		.NET Framework 3.5 SQL Server 2005 Express (optional)
Browser		Internet Explorer 7.0 or later
Note: The software programs End-User Runtimes (November 2008) and .NET Framework 3.5 are necessary to run the GV-ASManager. The software programs can be found in the accompanying software CD.		

2.2 Installing the GV-ASManager

Starting from version 2.0.1, the GV-ASManager software coming with GV-AS Controller can manage one controller. If you need to manage more than one controller, it is necessary to use the USB dongle with the GV-ASManager software. The available types of dongles for purchase are as follows:

USB Dongle for GV-ASManager

- **Dongle 4** is used for connection of up to 4 GV-AS Controllers.
- **Dongle 10** is used for connection of up to 10 GV-AS Controllers.
- **Dongle 30** is used for connection of up to 30 GV-AS Controllers.
- **Dongle 50** is used for connection of up to 50 GV-AS Controllers.
- **Dongle 255** is used for connection of up to 255 GV-AS Controllers.

USB Dongle for Connecting IP Cameras

Starting from GV-ASManager 3.0, no USB dongle is needed to connect to IP cameras.

To install the USB Dongle drivers:

1. Insert the USB Dongle to your computer.
2. Insert Software CD to your computer and a window will pop up automatically. Select **Install or Remove GeoVision GV-Series Driver** and click **Install Geovision USB Devices Driver**.

To install the GV-ASManager:

The **GV-ASManager V2.0 or later** must run with DirectX End-User Runtimes (November 2008) and .NET Framework. Follow these steps to install the programs.

1. Insert Software CD to your computer and a window will pop up automatically.
2. If you don't have DirectX 9.0c installed in your computer, select **Install DirectX 9.0c**.
3. Select **Install DirectX End-User Runtimes (November 2008)**.
4. Select **Install Microsoft .NET Framework Version 3.5**.
5. Select **Install GeoVision V3.0.0.0 Access Control System**, click **GeoVision Access Control System** and follow on-screen instructions to complete the installation.

2.3 Logging in

Before using the GV-ASManager, you need to set the login ID and password, and create a database.

1. Click **Start**, point to **Programs**, select **Access Control** and click **ASManager**. When you start the system for the first time, the system will prompt you for a Supervisor ID and Password as below.

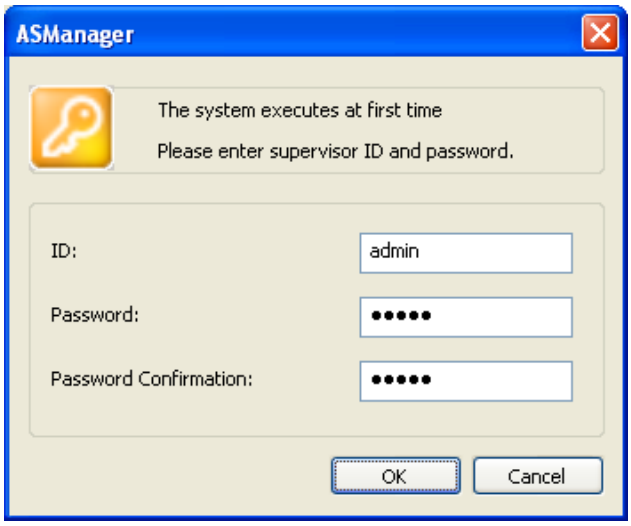


Figure 2-1

2. Type a name you wish to be the Supervisor in the ID field and type the password.
3. Click **OK**. The message "*Can't open database. Would you like to set up database?*" appears.
4. Select **Yes** to create a database. The ID and password you have configured in Step 1 are required to access the feature. This dialog box appears.

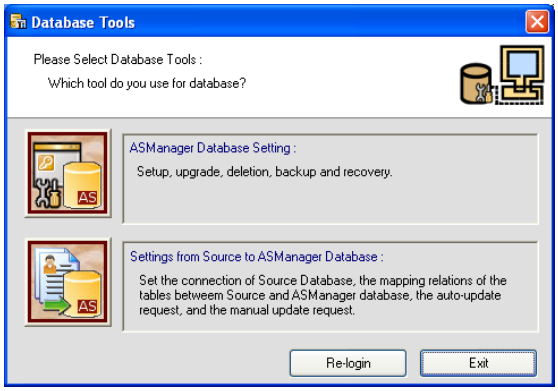

Database Tools
Please Select Database Tools :
Which tool do you use for database?
ASManager Database Setting :
Setup, upgrade, deletion, backup and recovery.
Settings from Source to ASManager Database :
Set the connection of Source Database, the mapping relations of the tables betweem Source and ASManager database, the auto-update request, and the manual update request.
Re-login
Exit

Figure 2-2

5. Select **ASManager Database Setting**. The ASManager Database Setting dialog box appears.

6. You can create either a Microsoft Access database or a Microsoft SQL database. To create a Microsoft SQL database, see *Chapter 12 Database Settings*. To create a Microsoft Access database:

   - **For the first-time user of GV-ASManager:**

   Select **Setup MDB / MSSQL Database for ASManager**. The Setup Database Connection dialog box appears. Select **Microsoft Office Access Database**, and click **OK**. The program starts creating a database. When it is complete, the message "*Setup database connection successfully*" will appear.

   - **For the user upgrading GV-ASManager version to 3.0 or later:**

   Select **Upgrade to Latest Database Version**. The program starts upgrading the old database. When it is complete, the message "*Upgrade database successfully*" will appear.

7. Restart **ASManager**. You can see the main screen of the GV-ASManager.

Note:

1. After you upgrade GV-ASManager, it is recommended to also upgrade the GV-AS Controller firmware. To upgrade the controller firmware, use the **Update to the latest firmware version** function in the Net Module Utility. See *Chapter 13*.
2. By default the Access database is created at C:\Access Control\ASManager\ASRes.

Chapter 3 The Main Screen of GV-ASManager

After you run the GV-ASManager, the following main screen will appear. Get yourself familiar with the main screen, as it will help you when you read further in the following sections.

3.1 Main Screen

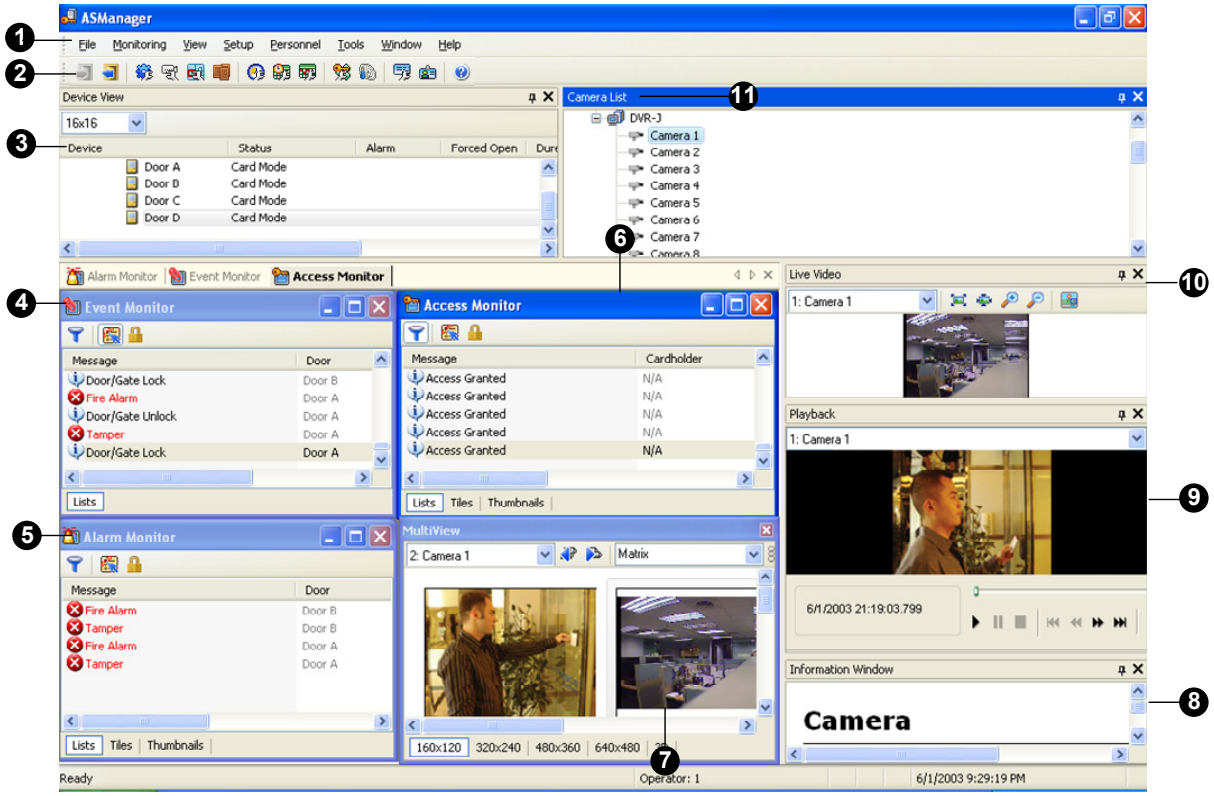


Figure 3-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of **File** (log in / out the GV-ASManager), **Monitoring** (display monitor windows of alarm, access and event), **View** (display the function windows), **Setup** (set up connected devices and schedules), **Personnel** (set up the cardholders' accounts), **Tools** (set up for notification and log) and **Window** (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of Login, Logout, Devices, Areas, Door Groups, Time Zones, Weekly Schedules, Holidays, Access Groups, Cards, Cardholders and About.

3	Device View	Displays a list of connected doors and their current status. You can change the size of icons to 16 x 16, 24 x 24 or 32 x 32 from the drop-down list.
4	Event Monitor	Displays monitored events of doors.
5	Alarm Monitor	Displays alarm events of doors.
6	Access Monitor	Displays access activities of doors.
7	MultiView	Displays live views of connected cameras from multiple IP devices. For details, see *5.4 The MultiView Window*.
8	Information Window	Displays the information of doors, card readers and monitored events.
9	Playback	Plays back recorded events from a compatible GeoVision IP device. For details, see *5.5 Retrieving Recorded Video*.
10	Live Video	Displays the live view of one connected camera. For details, see *5.2 Accessing a Live View*.
11	Camera List	Displays a list of connected cameras.

Note: After closing the main screen, GV-ASManager will continue to run in **Windows Task Manager**.

3.1.1 Toolbar

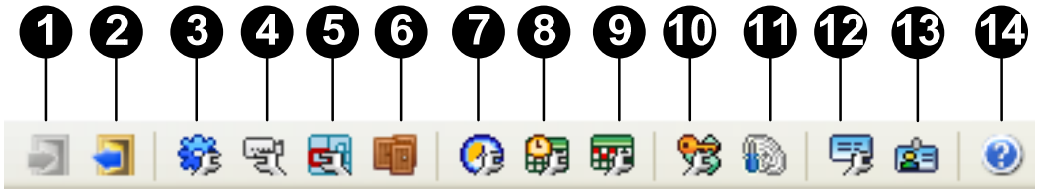


Figure 3-2

The buttons on the Toolbar of GV-ASManager:

No.	Name	Function
1	Login	Logs in the GV-ASManager.
2	Logout	Logs out the GV-ASManager.

3	Devices	Defines controllers and doors.
4	Cameras	Searches the GV IP devices on the same network. For details, see *Chapter 5 Video Integration*.
5	Areas	Configures Global Anti-Passback. For details, see *6.3 Global Anti-Passback.*
6	Door Groups	Assigns controllers into door groups to be able to quickly upload fingerprints to multiple controllers. For details, see *7.4.4 Uploading Fingerprints to Controllers Using Door Groups*.
7	Time Zones	Defines the minutes and hours of the day when a user is granted access to a secure site. For details, see *4.4.1 Step 1: Setting Time Zones*.
8	Weekly Schedules	Defines the days of the week when a user is granted access to a secure site. For details, see *4.4.2 Step 2: Setting Weekly Schedules*.
9	Holidays	Defines the specific dates as holidays. For details, see *4.4.3 Step 3: Setting Holidays*.
10	Access Groups	Sets up different groups to define who can access what door at what time of a day. For details, see *4.5 Setting Access Groups*.
11	Fingerprint Access	Uploads the enrolled fingerprints to the controllers. For details, see *7.4.3 Uploading Fingerprints to Controllers*.
12	Cards	Creates and edits a database of card information. For details, see *4.3 Setting Cards*.
13	Cardholders	Creates and edits a database of cardholder information. For details, see *4.6 Setting Cardholders*.
14	About	Displays the version of GV-ASManager.

3.2 Device View

The Device View displays the activity and status of the connected doors.

- To open the Device View window, click **View** on the menu bar and select **Device View**.

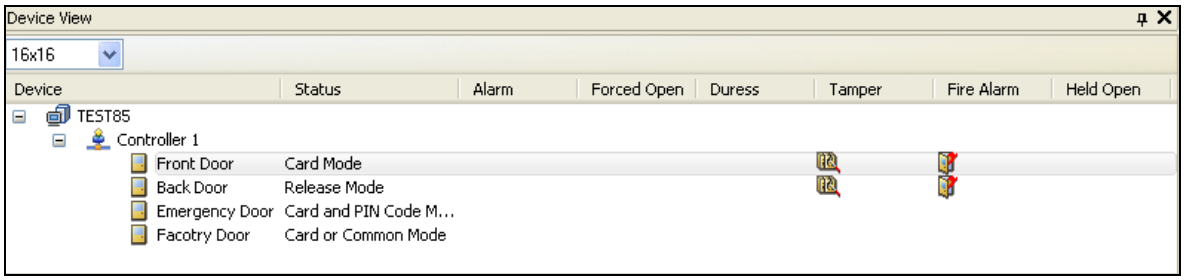


Figure 3-3

3.2.1 Controls on the Window

You can control a connected controller or door by right-clicking it in the Device View window.

The menu options of the **Host** include:

Name	Function
Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation	Controls the behaviors of all doors associated with the server. The options of **Force Unlock** and **Force Lock** will let the door stay open or locked until you select **Disable Door Lock Operation**. The **Unlock Door** option will let the door open temporarily until the specified time is expired. See “Lock Reset Time” at Step 2 in *4.2.2 Step 2: Configuring a Door*.
Reset Anti-Passback	Clicking this option enables a user to re-access the entry or exit reader. See *Chapter 6 Anti-Passback*.

The menu options of the **Controller** include:

Name	Function
Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation	Controls the behaviors of all doors associated with the controller. The options of **Force Unlock** and **Force Lock** will let the door stay open or locked until you select **Disable Door Lock Operation**. The **Unlock Door** option will let the door open temporarily until the specified time is expired. See “Lock Reset Time” at Step 2 in *4.2.2 Step 2: Configuring a Door*.
Reset Anti-Passback	Clicking this option enables a user to re-access the entry or exit reader. See *Chapter 6 Anti-Passback*.
Reconnect	Reconnects with the controller.
Sync Controller	After the controller settings are modified, clicking **Sync Controller** can immediately renew the settings.
Settings	Modifies the controller settings in the Controller Setup dialog box.

The menu options of the **Door** include:

Name	Function
Unlock Door, Force Unlock, Force Lock, Disable Door Lock Operation	Controls door behaviors. The options of **Force Unlock** and **Force Lock** will let the door stay open or locked until you select **Disable Door Lock Operation**. The **Unlock Door** option will let the door open temporarily until the specified time is expired. See “Lock Reset Time” at Step 2 in *4.2.2 Step 2: Configuring a Door*.
Clear Alarm, Clear Force Open, Clear Duress, Clear Tamper, Clear Fire Alarm, Clear Held Open, Clear Access Denied	Clears the alarm conditions. The **Clear Alarm** option refers to clear alarm sounds. For alarm settings, see Step 5 in *4.2.2 Step 2: Configuring a Door*.
Sync GeoFinger	If fingerprint data failed to upload to the controllers, click **Sync GeoFinger** to re-upload the selected fingerprint data.
Settings	Modifies the controller settings in the Controller Setup dialog box.

3.3 Monitoring Windows

Three monitoring windows are provided for users to oversee different types of door activities: Access Monitor, Alarm Monitor and Event Monitor.

- To open these windows, click **Monitoring** on the menu bar, and select the desired windows.

3.3.1 Controls on the Window

The three monitoring windows of Access Monitor, Alarm Monitor and Event Monitor have the same controls on the window.

We use the Access Monitor window as example to explain the controls.

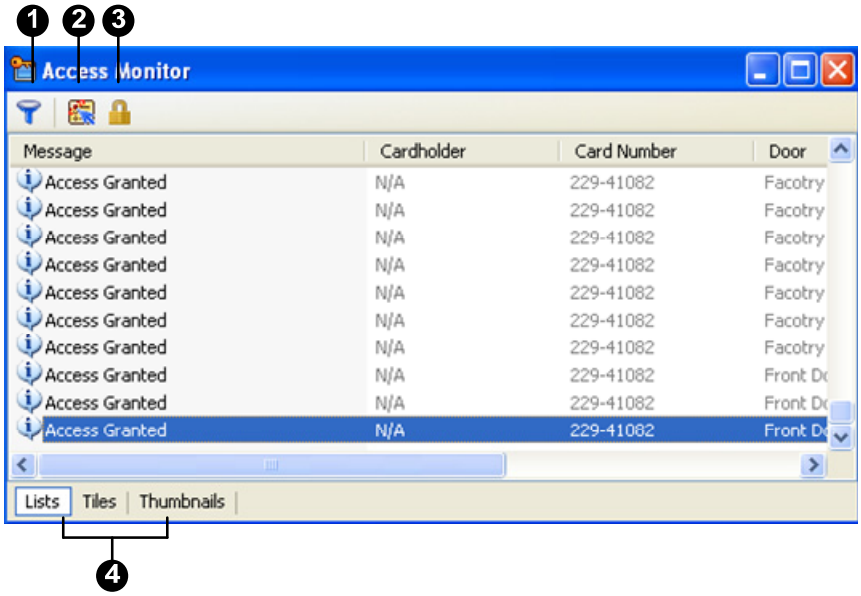


Figure 3-4

No.	Name	Function
1	Filter	Sets up criteria to only display the desired activity information.
2	Auto Select	Focuses on the latest data display.
3	Lock	Suspends the current data display.
4	Lists / Tiles / Thumbnails	Decides how events are displayed on the window.

The following options are only accessible on the **Access Monitor** window. Right-clicking one message allows you to access its detailed information.

Name	Function
New/Edit Card	Enrolls a new card or edits the card information.
Browse Card Information	Views the card information.
Browse Cardholder Information	Views the cardholder information.
Show Image	If the camera monitors when the activity happened, the related image is available.

3.3.2 Customizing a Monitoring Window

You can customize the messages displayed on a monitoring window by defining filter criteria. Multiple custom monitoring windows can be added for your specific requirements.

1. To add one monitoring window, click **Monitoring** on the menu bar. Then select **New Alarm Monitor**, **New Access Monitor** or **New Event Monitor**.
2. Click the **Filter** button on the monitoring window. This dialog box appears.

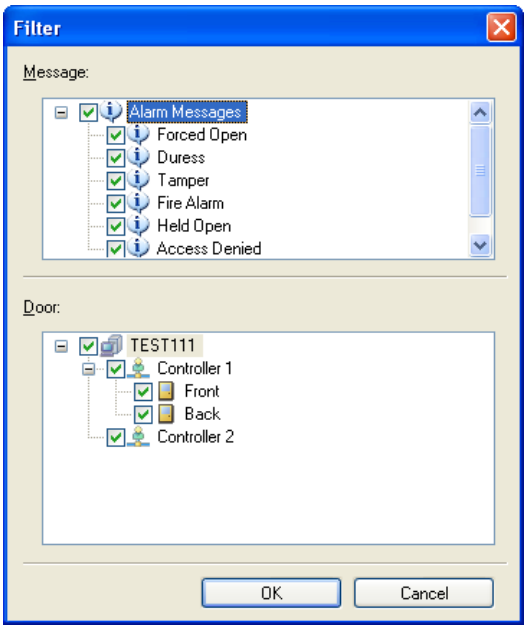


Figure 3-5

3. Select the desired messages and devices for monitoring, and click **OK**. The monitoring window will only display the messages based on the defined criteria.

4. Right-click the **Monitor** tab on the main screen, and select **Rename** to name the new monitoring window.

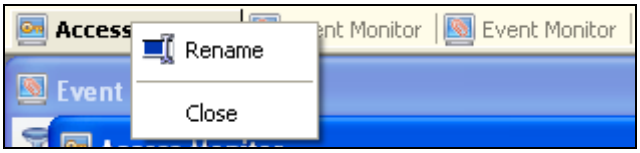


Figure 3-6

Note: The added windows are only for one-time use, and they cannot be saved after the monitoring window is closed.

3.3.3 Arranging Monitoring Windows

The monitoring windows can be arranged on screen in several ways.

On the menu bar, click **Window**, and select one of the following options to arrange the windows:

- **Cascade:** Overlaps the open windows and shows their title bars.
- **Tile Horizontally:** Arranges the open windows horizontally.
- **Tile Vertically:** Arranges the open windows vertically.
- **Arrange Icons:** Arranges the minimized windows on the bottom.

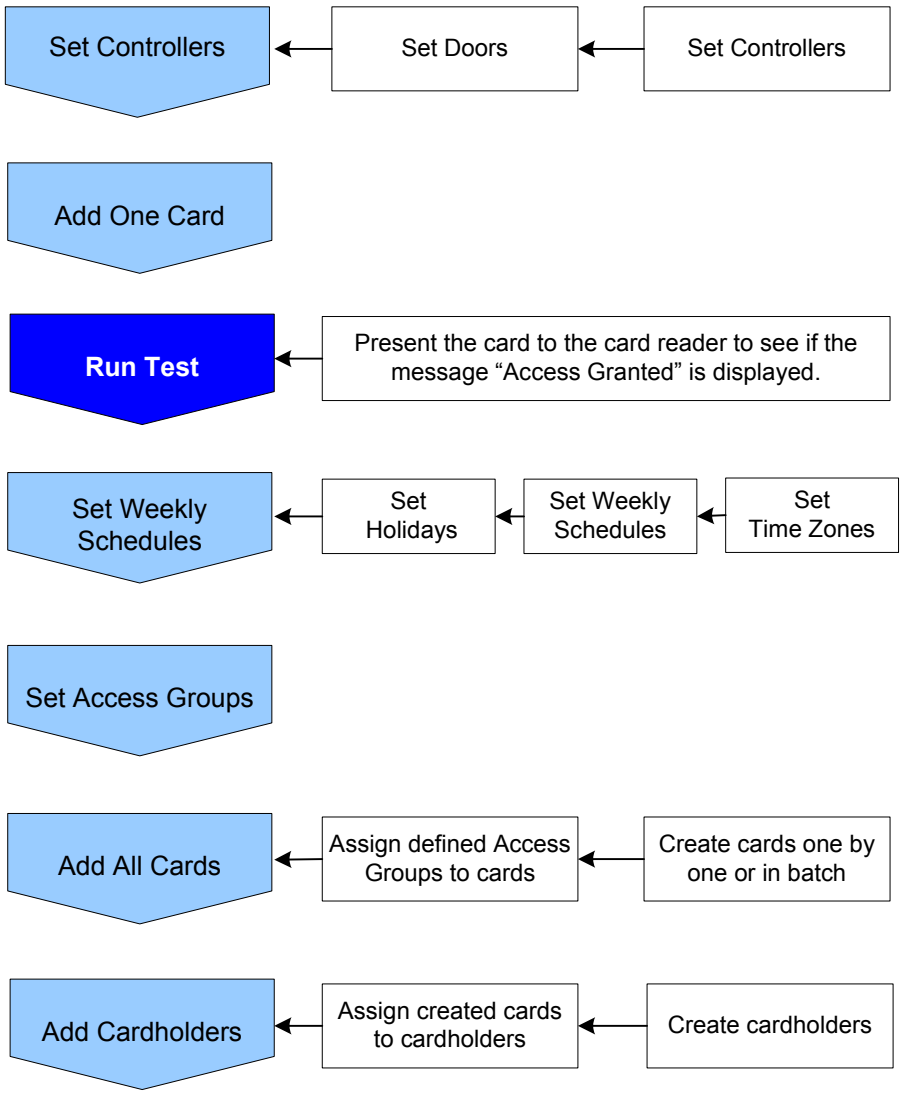
Chapter 4 Settings

This section describes the following settings:

- Setting Controllers
- Setting Cards
- Setting Weekly Schedules
- Setting Access Groups
- Setting Cardholders

4.1 Setup Flowchart

To get started quickly with GV-ASManager settings, follow the process illustrated below.



4.2 Adding Controllers

To add the GV-AS Controller to the GV-ASManager, follow these steps:

- **Step 1 Configuring a Controller**

  Establish the communication between the GV-AS Controller and GV-ASManager.

- **Step 2 Configuring a Door**

  Define the doors on a door controller.

4.2.1 Step 1: Configuring a Controller

1. On the menu bar, click **Setup** and select **Device**. The Controller List dialog box appears.
2. Click the **Add** icon on the top left corner. This dialog box appears.

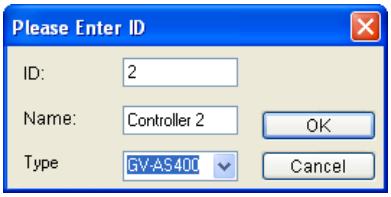


Figure 4-1

3. Enter **ID** and **Name** of the Controller, select **Type** of the Controller and click **OK**. This dialog box appears.

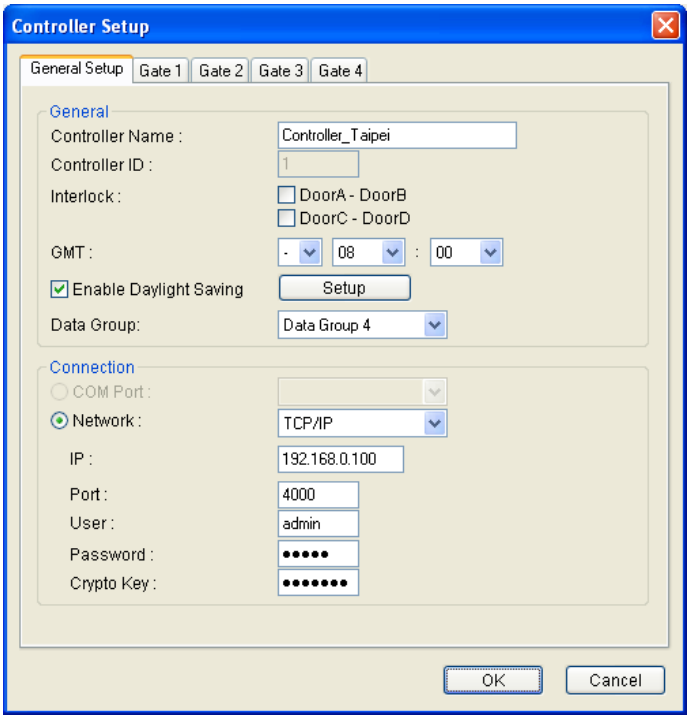


Figure 4-2

Note: The Controller ID is set ahead with GV-ASKeypad or Web interface. Refer to *GV-AS Controller Installation Guide*.

4. In Connection section, select the communication mode between the GV-AS Controller and GV-ASManager.
   - If using RS-485 connection, select **COM Port** that is used for connection.
   - If using Ethernet, select **Network** and select **TCP/IP** or **LocalDDNS**. Type the IP address, device name (if LocalDDNS is selected), port number, login user, login password and Crypto key (3DES code) of the GV-AS Controller.

Note: The default values of GV-AS Controller are: IP address **192.168.0.100**; username **admin**; password **admin**; Crypto key (3DES code) **12345678**.

5. To check if the above connection settings are correct, you can click **OK** at this step and back to the main screen. The icon appearing on the Device View window indicates the connection is established.

Note: For the disconnection messages displayed on the Status column (Figure 4-5), see *D. Controller Status* in *Appendix*.

6. OPTIONAL settings in the General section:
   - **Interlock:** Enable the “interlocking” feature between two doors (Door A and Door B, or Door C and Door D). Doors that are interlocked cannot be open at the same time. One door unlock only when the other door is close.
   - **GMT:** The current time at the host computer.
   - **Enable Daylight Saving:** Enable the Daylight Saving feature. The system will automatically adjust for daylight saving time.
   - **Data Group:** Assign the controller to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 7 for more details.

4.2.2 Step 2: Configuring a Door

1. To define the doors on the controller, click the **Door/Gate** tab. This dialog box appears.

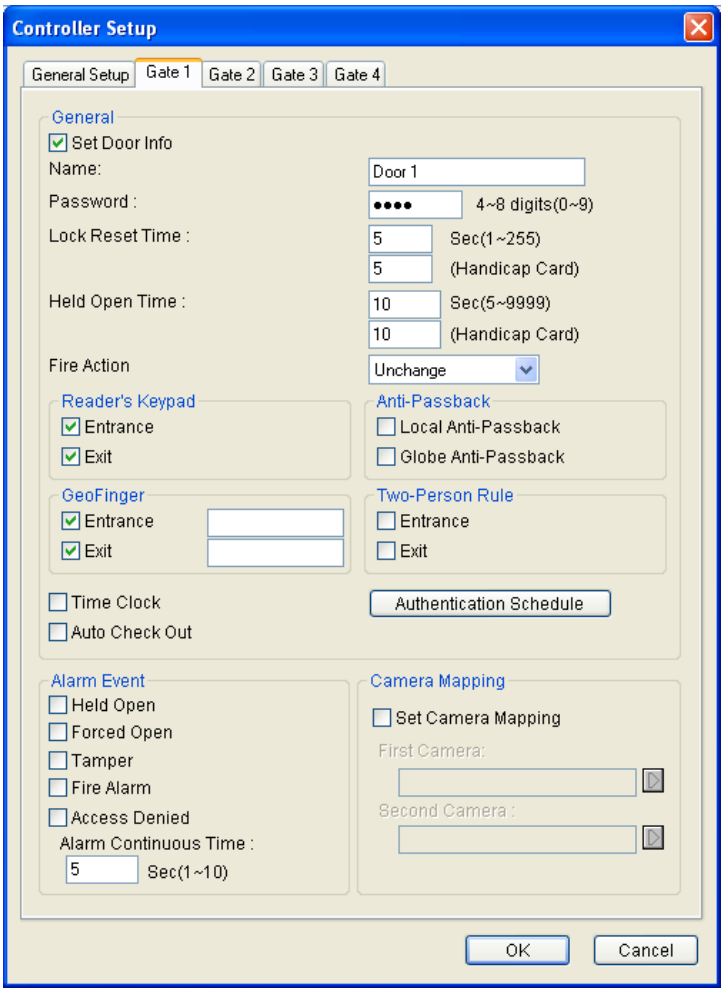


Figure 4-3

2. In the General section, enable **Set Door Info** to define the general parameters for the door:

   - **Name:** Give a name to the door.
   - **Password:** Give a password to the door. The default setting is 1234.
   - **Lock Reset Time:** If the door is monitored, type the number of seconds the door can be held open. After the specified time expired, the door will automatically be locked. Next to **Handicap Card**, type the number of seconds the door will be held open when a Handicap Card is swiped.
   - **Held Open Time:** If the door is monitored, type the number of seconds the door can be held open before a Door Held Open alarm is generated. Next to **Handicap Card**, type the number of seconds the door can be held open after a Handicap Card is swiped before a Door Held Open alarm is generated.

- **Fire Action:** Set the door to be locked or unlocked when a fire alarm condition occurs.

3. The following settings are OPTIONAL and are only applicable when related settings are also configured:
   - **Reader's Keypad:** When the Card and PIN Code Mode is applied, normally both the access card and PIN code are required. But if the **Entrance** or **Exit** option is not selected, only the access card is required to unlock the door. For example, if only the **Entrance** option is selected, the user will be required to both present the card and enter the PIN code to unlock the entry door, but only the card will be required to unlock the exit door. To apply Card and PIN Code mode, see step 4 below.
   - **Anti-Passback:** To perform the Anti-Passback application, see *Chapter 6 Anti-Passback*.
   - **GeoFinger:** Enables fingerprint authorization if the door is installed with GV-GF Fingerprint Readers. To enable fingerprint authorization for both exit and entrance doors, select both **Exit** and **Entrance**.
   - **Two Person Rule:** Select **Entrance** to require presenting Two Person A Card and then Two Person B Card before the entry door is unlocked. Select **Exit** to require presenting both cards in the right order before the exit door is unlocked. To set a card as Two Person A/B Card, see *Adding a Single Card* section later in this chapter.
   - **Time Clock:** This option must be selected to enable GV-TAWeb. See *Chapter 10 GV-TAWeb for Workforce Schedule* for more details.
   - **Auto Check Out:** Automatically checks out the Visitor Card when the visitor presents the card at the exit door. To set a card as Visitor Card, see *Adding a Single Card* section later in this chapter.

4. The **Authentication Schedule** is an OPTIONAL setting for specifying different access modes at different periods of time; otherwise the default access mode is **Card Mode** that requires users to present the card only to be granted access.

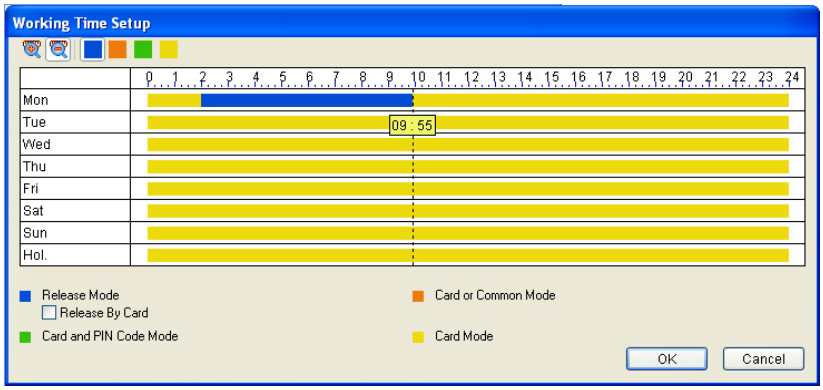


Figure 4-4

To define which kind of access mode should be applied at specific day and time, select one access mode on the toolbar and drag the mouse over the timelines. Four (4) access modes are available in the system:

- **Card Mode:** This is the default mode. This mode only requires the user to present his or her card to be granted access.
- **Release Mode:** Keep the door in an unlock status with the reader.
  - **Release by Card:** The door will unlock only after a card is presented and will remain unlocked during the time specified for Release Mode. This option is designed to prevent unattended doors from opening during the Release Mode time.
- **Card and PIN Code Mode:** This mode requires the user to present his or her card and then enter the card's PIN code on the keypad.
- **Card or Common Mode:** This mode requires the user to present his or her card to be granted access **OR** enter the door's password using the keypad to be granted access.

5. The settings in the Alarm Event section are OPTIONAL unless an alarm device is installed on the GV-AS Controller. Enable the desired alarm conditions that will cause the alarm to occur: **Held Open**, **Force Open**, **Tamper**, **Fire Alarm**, and **Access Denied**.
   - **Alarm Continuous Time:** Type the duration of the alarm sounds in seconds.
6. The settings in the Camera Mapping section are OPTIONAL unless a camera is installed at the secure site. For details see *Chapter 5 Video Integration*.
7. Click **OK** several times and return to the main screen. A controller folder tree will be displayed on the Device View window as example below.

   If the icon appears, it indicates the connection between the controller and GV-ASManager has been established.

   If the icon appears, it indicates the connection failed. Make sure the above connection setup is correctly configured.

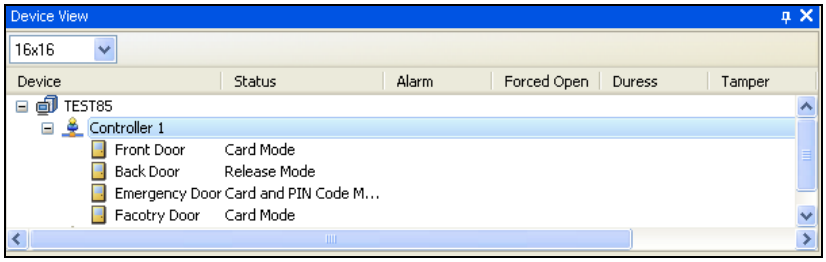


Figure 4-5

4.3 Setting Cards

Once you have configured the controller, you may start enrolling cards. All new cards must be enrolled into the GV-ASManager before access is allowed. Using GV-AS100, GV-AS110, GV-AS120 and GV-AS400, up to 40,000 cards can be stored. If a card that was not enrolled is presented to the reader, the message *Access Denied: Invalid Card* will be displayed.

Depending on how many cards you need to program, you can simply add them one at a time or use the batch function to add a group of cards.

4.3.1 Adding a Single Card

1. To add one card, use one of these ways:
   - Present the card to the reader. The message *Access Denied: Invalid Card* is displayed. Right-click the message and select **New/Edit Card**. The New a Card dialog box appears with card number and code type entered (Figure 4-7). Then follow Step 3 to complete other settings.
   - On the menu bar, click **Personnel** and select **Cards**. This window appears.

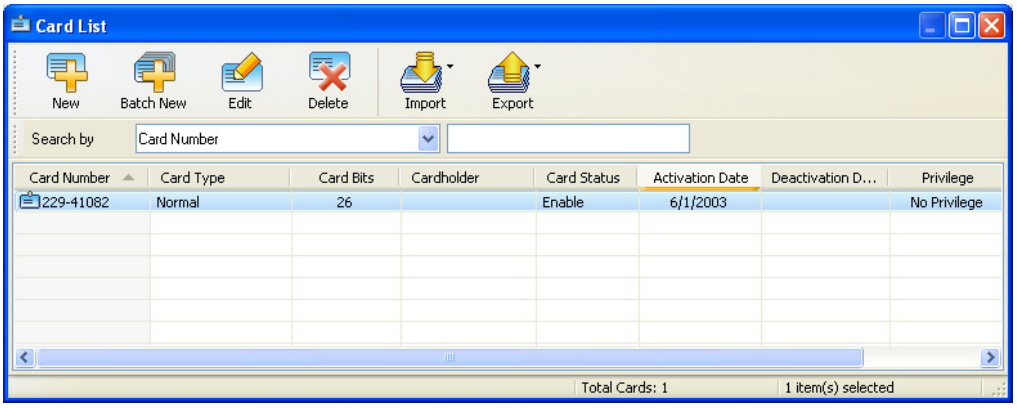


Figure 4-6

2. Click the **New** button on the toolbar. This dialog box appears.

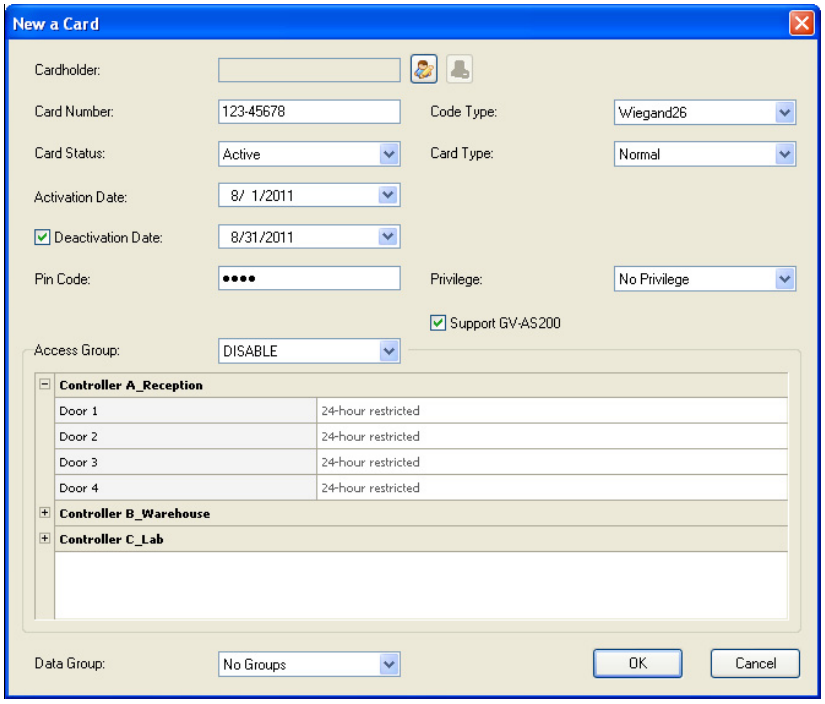


Figure 4-7

3. The settings are available for the card:

   - **Card Number:** Enter the card number.
   - **Code Type:** Select the code format of the card.
   - **Card Type:** Select one of the following card types.
     - **Normal:** The card opens the door when it is under Card Mode, the default mode.
     - **Patrol:** The card is assigned to the person in charge of patrolling a location, e.g. a guard. When the patrol card is presented to the reader, the access will be recorded but the door will NOT unlock. The feature may be set together with **Privilege** below. The patrol card user may have the privilege to stop alarm sounds and clear alarm events during patrolling.
     - **Two-person A Card:** Two-person A/B rule. The card is defined as Card A and Card B must be presented after Card A to unlock the two-person-rule enabled door.
     - **Two-person B Card:** Two-person A/B rule. The card is defined as Card B and Card A must be presented before Card B to unlock the two-person-rule enabled door.
     - **Visitor:** This card is assigned to a visitor and the visitor's access can be managed using GV-VMWeb.

- **Security:** The security card can enable the Security Mode where no cards can be granted access. Only the security card can disable the Security Mode.
- **Handicap:** When the handicap card is used, the door will remain unlocked for the time specified in Lock Reset Time and Held Open Time for handicap card. To see how to set prolonged Lock Reset Time and Held Open Time for handicap card users, refer to *4.2.2 Step 2: Configuring a Door*.

- **Activation/Deactivate Date:** Specify when the card is active or inactive.
- **PIN Code:** Enter a four-digit personal code for the card. The default setting is 1234.
- **Privilege:** Assign one of these privileges to the cardholder:
  - **Stop Alarm:** The cardholder can stop alarm sounds by presenting the card.
  - **Clear Event:** The cardholder can clear alarm events by presenting the card. All alarms in the Device View window are erased. A record of these alarms is still kept in the Alarm Monitor.
- **Support GV-AS200:** If the GV-ASManager is connected to GV-AS200 and other types of GV-AS Controllers simultaneously, select this option so that the first 10,000 card data can be shared for use between GV-AS200 and another type of GV-AS Controller.
- **Access Group:** Access Groups control which personnel can access which door and at what time. For details, see *4.5 Setting Access Groups.*

  For first-time user of the GV-ASManager, the access group is not yet established. Select **User Define** for test run.
- **Controller:** The Controller column displays the associated doors. The selection for each door will be automatically brought up when one access group was entered.

  For first-time user of the GV-ASManager, select **24-hour access** for each door for test run.
- **Data Group:** Assign the card to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions listed under the data group. Refer to *Adding a New User* in Chapter 7 for more details.

4. Present the enrolled card to the reader. Once the card has been accepted, the message *Access Granted* will be displayed.

4.3.2 Adding a Group of Cards

Before you use the Batch function to enroll new cards, please note that the group of cards must be numbered sequentially.

1. On the menu bar, click **Personnel** and select **Cards.** The Card List dialog box appears.
2. Click the **Batch New** button on the toolbar. This dialog box appears.

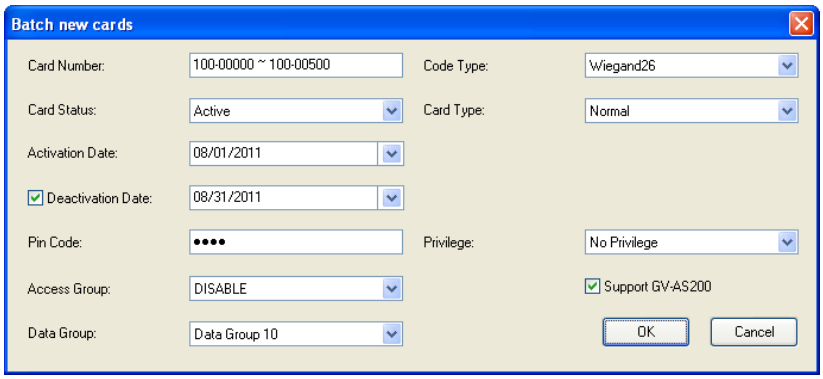


Figure 4-8

3. The settings in the dialog box are the same as those of adding a single card. See Step 3 in *4.3.1 Adding a Single Card*.

Note: Cards that were enrolled using the Batch function will have the same PIN. If you want to change the PINs of certain cards, you have to enter the PIN using the **Edit** function on the Card List dialog box.

4.3.3 Importing/Exporting Card Data

You can import and export card data in mdb or xls format.

To export card data:

1. On the Card List window (Figure 4-6), select desired cards using Ctrl + left click.
2. Click the **Export** button and select **Export to Access** or **Export to Excel**.
3. Assign the file path, and optionally enter password to export card data.

Note: The Excel file format does not support the password protection.

To import card data:

1. On the Card List window (Figure 4-6), click the **Import** button and select one of these options: **Import from Access** or **Import form Excel**.
2. Assign the file path and enter **Password** if necessary. Click **OK**. This dialog box appears.

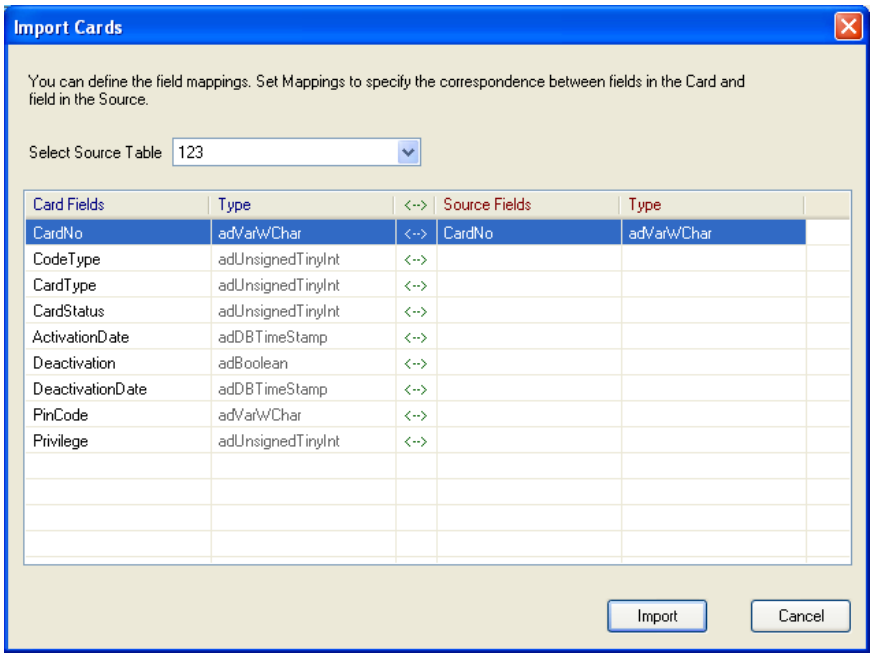


Figure 4-9

3. Select desired **Source Table**, and click the columns under **Source Fields** to enable the selection. Select the corresponding source items to map between Source Fields and Card Fields.
4. Click **Import** to import card data.

4.4 Setting Weekly Schedules

This section will help you define the daily and holiday access times. Up to 254 weekly schedules may be defined with two default weekly schedules for “deny access” and “full access”.

Before creating weekly schedules, it is helpful to map out all possible usages of weekly schedules for the site. For example: consider the variety of access hours for employees, consider requirements for janitorial personal who may need night access, consider requirements for service or repair personnel who may need all hours access, consider requirements for supervisory staff who may need extended hours access and etc.

- **Step 1 Setting Time Zones**

  Define the minutes and hours of the day when a user is granted access to a secure site. The minimum time duration is 5 minutes.

- **Step 2 Setting Weekly Schedules**

  Define the days of the week when a user is granted access to a secure site.

- **Step 3 Setting Holidays**

  Define specific dates as holidays.

4.4.1 Step 1: Setting Time Zones

This section provides examples of setting the following time zones:

- Day shift – 09:00 to 19:00 hours
- Night shift – 19:00 to 9:00 hours (cross midnight)
- Supervisor – 07:00 to 24:00 hours

1. On the menu bar, click **Setup** and select **Time Zones**. This dialog box appears.

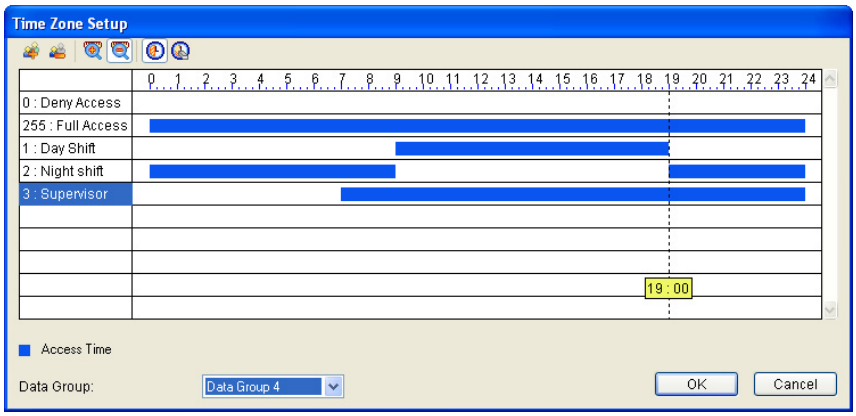

Time Zone Setup
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
0 : Deny Access
255 : Full Access
1 : Day Shift
2 : Night shift
3 : Supervisor
19 : 00
Access Time
Data Group:
Data Group 4
OK
Cancel

Figure 4-10

2. Click the **Add** button . This dialog box appears.

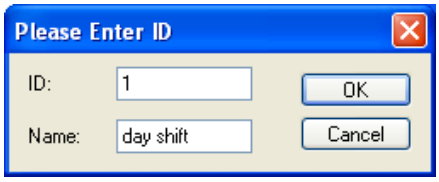


Figure 4-11

3. The **ID** is the number of the time zone. The system will automatically create the ID based on how many time zones have been added. Give a **Name** to the time zone you are going to define. Click **OK**.

   For example, name the Time Zone 1 as **day shift**.

4. Click the **Add Access Time** button . Then drag the mouse on the timeline to define a period of access time.

   For example, the time of day shift is **from 09:00 to 19:00**.

5. To create the second time zone, click the **Add** button and name it as **night shift**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 19:00 to 24:00** and **from 00:00 to 09:00**.

6. To create the third time zone, click the **Add** button and name it as **Supervisor**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 07:00 to 24:00**.

7. You can use the **Data Group** drop-down list to assign the time zone to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 7 for more details.

8. Click **OK**. The three time zones have been defined.

4.4.2 Step 2: Setting Weekly Schedules

This section provides examples of setting the following weekly schedules:

- Schedule-Day shift – Monday through Friday, 09:00 to 19:00 hours
- Schedule-Night shift – Monday through Friday, 19:00 to 9:00 hours
- Schedule-Supervisor – Monday through Sunday and Holidays, 07:00 to 24:00 hours

1. On the menu bar, click **Setup** and select **Weekly Schedules**. This dialog box appears.

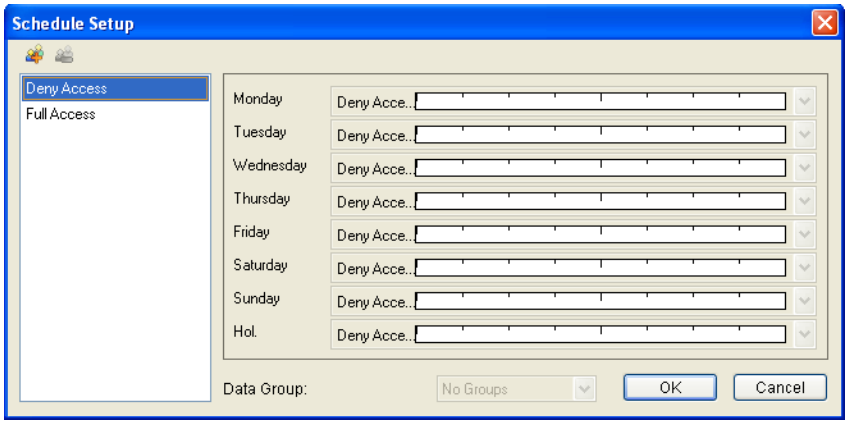


Figure 4-12

2. Click the **Add** button. This dialog box appears.

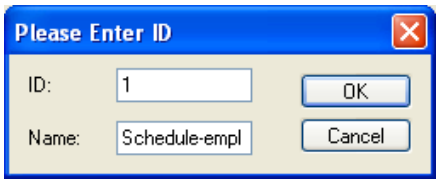


Figure 4-13

3. The **ID** is the number of the weekly schedule. The system will automatically create the ID based on how many time schedules have been added. Give a **Name** to the weekly schedule you are going to define. Click **OK**.

   For example, name the Weekly Schedule 1 as **Schedule-Day shift**.

4. From the drop-down lists of **Monday** to **Friday**, select the **Day shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.

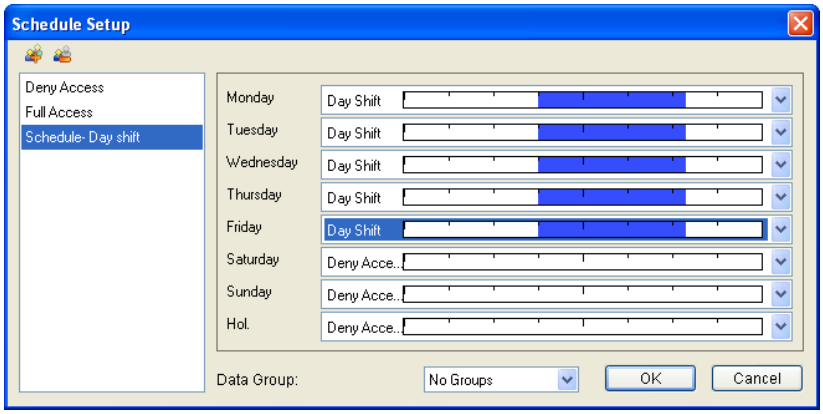


Figure 4-14

5. To create the second time schedule, click the **Add** button and name it as **Schedule-Night shift**. From the drop-down list of **Monday** to **Friday**, select the **Night shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.

6. To create the third time schedule, click the **Add** button and name it as **Schedule-Supervisor**. From the drop-down lists of **Monday** to **Hol**, select the **Supervisor** time zone we have created.

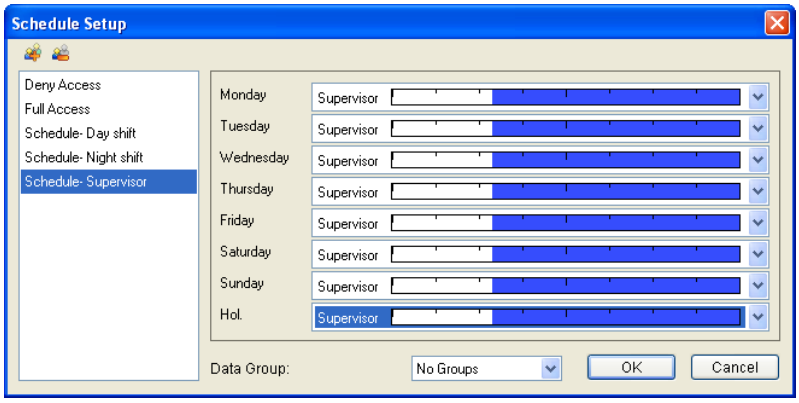


Figure 4-15

7. You can select a time schedule and use the **Data Group** drop-down list to assign the time schedule to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 7 for more details.

8. Click **OK.** The three weekly schedules have been defined.

4.4.3 Step 3: Setting Holidays

To designate specific dates as holidays on the system:

1. On the menu bar, click **Setup** and select **Holidays**. This dialog box appears.

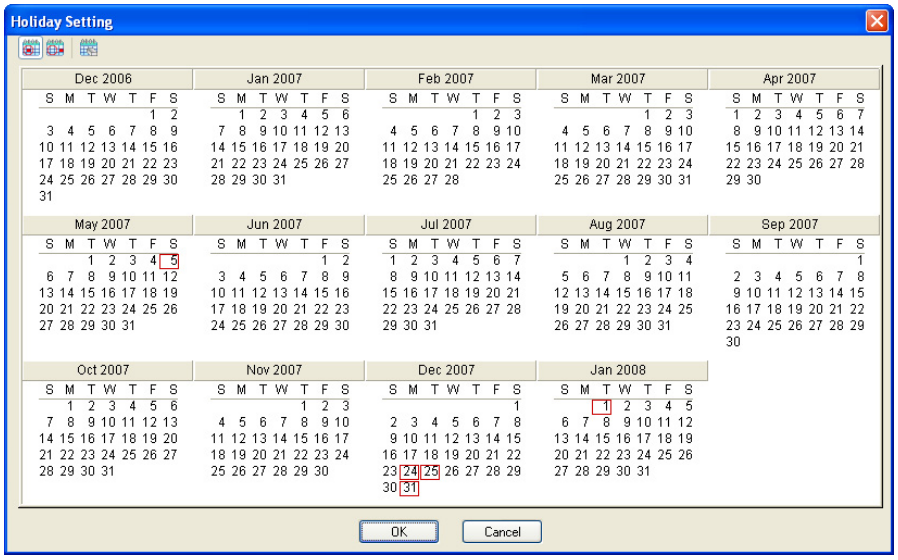


Figure 4-16

2. Click the **Holiday** icon and click the dates you want to set as holidays. For example,
   - Dec 24, 2007 – Christmas Eve
   - Dec 25, 2007 – Christmas Day
   - Dec 31, 2007 – New Year's Eve
   - Jan 01, 2008 – New Year's Day
3. To delete the holiday, click the **Non Holiday** icon and click the date you want to delete.

Note: Holiday dates can cross over to the following year, and certain holiday dates change from year-to-year. Administrators should review and update the holiday setting prior to the beginning of a new year to ensure proper holiday coverage.

4.5 Setting Access Groups

Access groups restrict which personnel can access which door, and at what time and day. To be granted access to a secure door, a user must meet the criteria of the access group. The user must be at a door that accepts the members of that access group, and it must be during a weekly schedule that allows that user access.

This section uses an example to describe how to create an access group and assign the criteria of the access group to a card. In this example, the FAE staff of day shift needs access to the front and back doors during the day shift time.

1. On the menu bar, click **Setup** and select **Access Groups**. This dialog box appears.

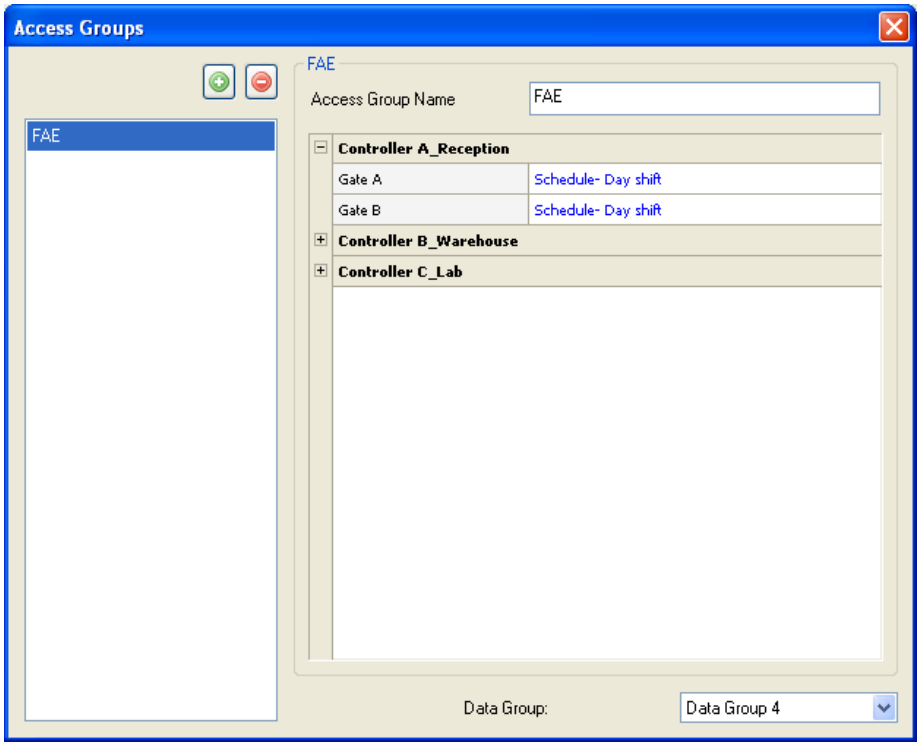


Figure 4-17

2. Click the **New** button , and give a **Name** to the new access group.

   For example, name the access group as **FAE**.

3. To define door access for the access group, click the drop-down list of each door and select one of pre-defined Weekly Schedules.

   For example, click the blue fields of **Gate A** and **Gate B**, and then select **Schedule-Day shift**.

4. You can use the **Data Group** drop-down list to assign the access group to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 7 for more details.
5. Click **OK**. The access group for the FAE staff has been created.
6. To assign the criteria of the access group to a single card, click **Personnel** on the menu bar and select **Cards**. The Card List dialog box appears.
7. Double-click one listed card. This dialog box appears.

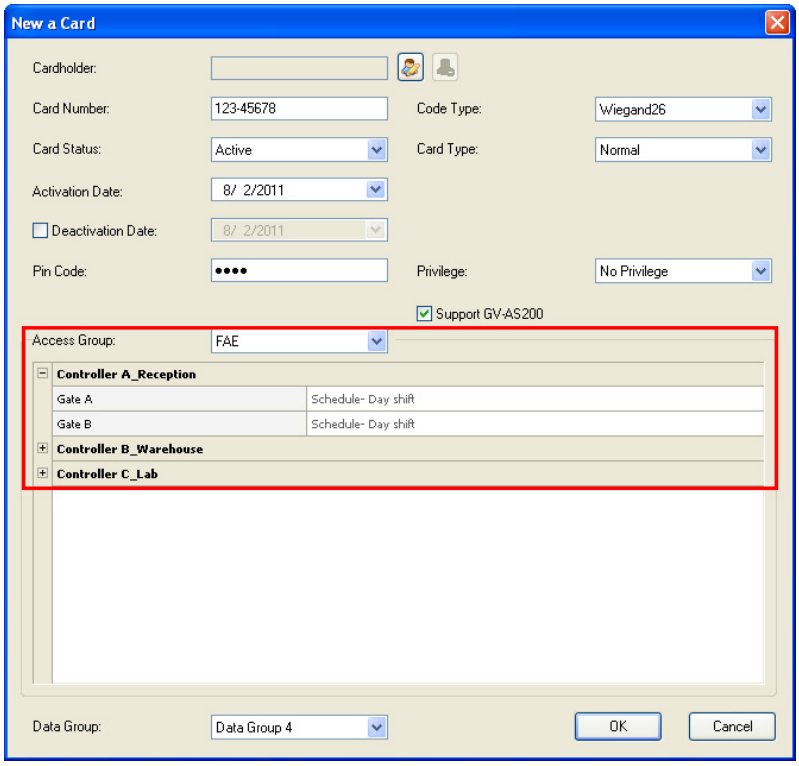


Figure 4-18

8. From the **Access Group** drop-down list, select one pre-defined access group, e.g. **FAE**. The assigned Weekly Schedule will be displayed on the associated door's field.

4.6 Setting Cardholders

This section describes how to create a database of cardholder information, and assign cards to cardholders.

4.6.1 Adding a Cardholder

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Click the **New** button on the toolbar. This dialog box appears.

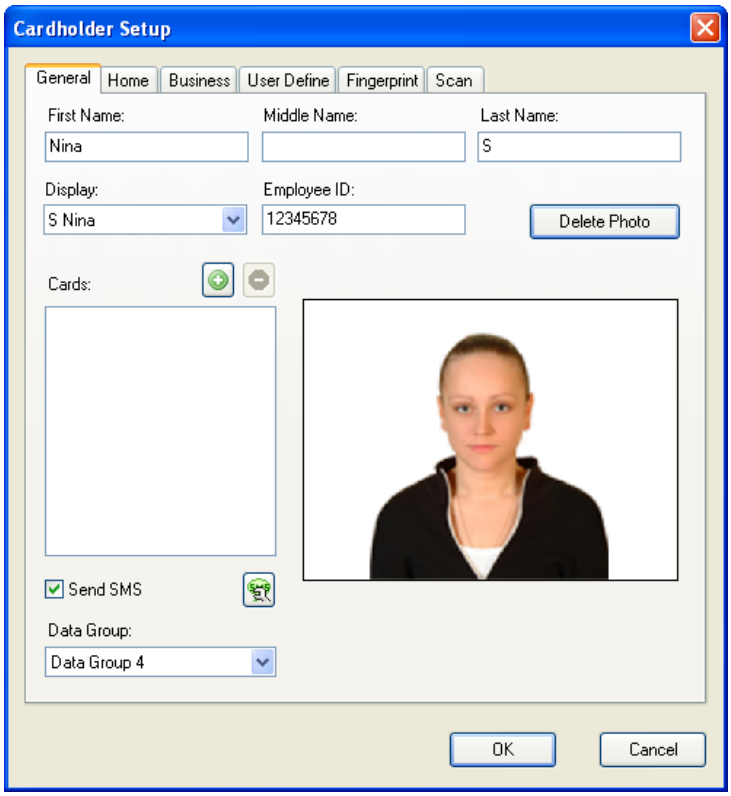


Figure 4-19

3. Type a name under **Display**, which is a required field. Other information of the cardholder such as Employee ID, Photo, Home information and Company information are optional entries.
4. You can use the **Data Group** drop-down list to assign the cardholder to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 7 for more details.

4.6.2 Assigning a Card to a Cardholder

There are two methods to assign a card to a cardholder.

Note: At this step we assume that you have followed the instructions in *4.3 Setting Cards* to complete your card enrollment.

---

1. On the Cardholder Setup dialog box (Figure 4-19), click **Add** and double-click one listed card to assign the card to the cardholder.

2. On the Edit Card dialog box (Figure 4-18), click the **Assign Cardholder** icon and double-click one listed cardholder to assign the cardholder to that card.

4.6.3 Sending SMS Alerts

If you want to send SMS alerts whenever the card(s) assigned to the cardholder is presented to the reader, select **Send SMS** in the Cardholder Setup dialog box.

Before sending the SMS, see *7.2.1 Setting SMS Server* to configure the SMS server. For how to set up SMS alerts, refer to the same settings “Send SMS Alert” at Step 3 in *7.2.3 Setting Notification*.

4.6.4 Customizing a Data Field

You can customize data fields for cardholders. Up to ten data fields can be created for user data entry.

When a custom data field is created, the field label will be displayed in the User Define tab on the Cardholder Setup dialog box. The actual personal data for each user is entered in the User Define tab.

To customize a data field:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Click the **User Define Fields Setting** button on the toolbar. The User Define Fields Setting dialog box appears.

3. Select one **User Define** field, and enter the text to be displayed as the field label. In this example, a Car License Plate field was created.

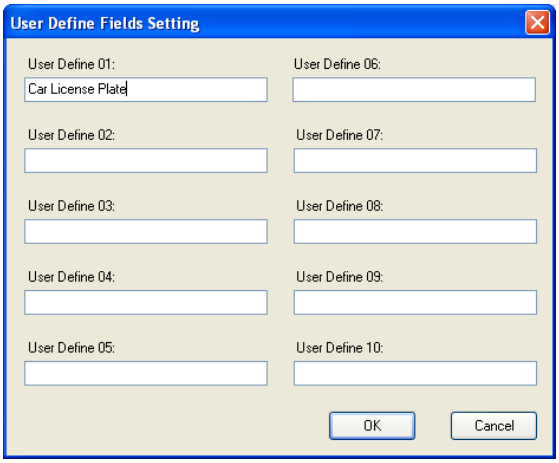


Figure 4-20

To enter personal data:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Double-click one listed user to whom personal data should be entered. The Cardholder Setup dialog box appears.
3. Click the **User Define** tab. The custom data field you have created now is displayed.
4. Click in the custom data field and enter the appropriate information. In this example, a number is entered in the created Car License Plate field:

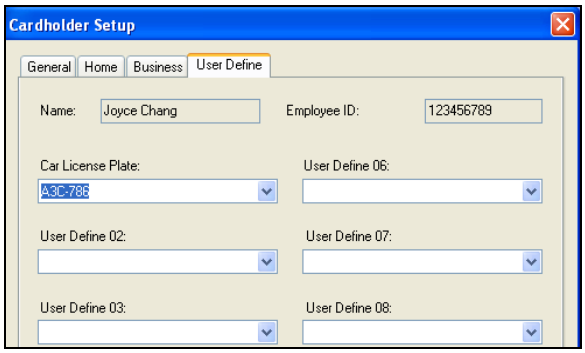


Figure 4-21

4.6.5 Importing/Exporting Cardholder Data

From the Cardholder List window, you can import and export cardholder data in mdb or xls format. For this function, please refer to *4.3.3 Importing/Exporting Card Data.*

Chapter 5 Video Integration

GeoVision IP devices and certain third-party IP cameras can be connected to the GV-ASManager through the network. Live video can then be accessed for monitoring and surveillance purposes.

The GV-ASManager provides the following video features:

- Live view
- Video playback
- Monitor up to 16 cameras at one time

Note:

1. GeoVision IP devices include GV-System, GV-NVR, GV-Video Server, GV-Compact DVR and GV-IP Camera. For compatible third-party IP cameras, see *Appendix A*.
2. To connect third-party IP cameras to GV-ASManager V2.3 and earlier versions, a NVR Dongle is required.
3. The GV-ASManager only supports GV-System of version 8.120 or later.
4. GV-Fisheye IP Camera is currently not supported on GV-ASManager.

Hint: In the following sections the term “DVR” refers to GV-System and GV-NVR, the term “Video Server” refers to GV-Video Server, and the term “Compact DVR” refers to GV-Compact DVR.

5.1 Mapping Cameras

If you want to map a camera from the DVR to a door, the DVR must be enabled for video access ahead:

- Enable **Control Center Server** (CCS)

To map cameras to a door:

1. On the menu bar, click **Setup** and select **Device**. The Controller List dialog box appears.
2. Double-click one listed controller. The Controller Setup dialog box appears.

3. Click one **Door** tab. This dialog box appears.

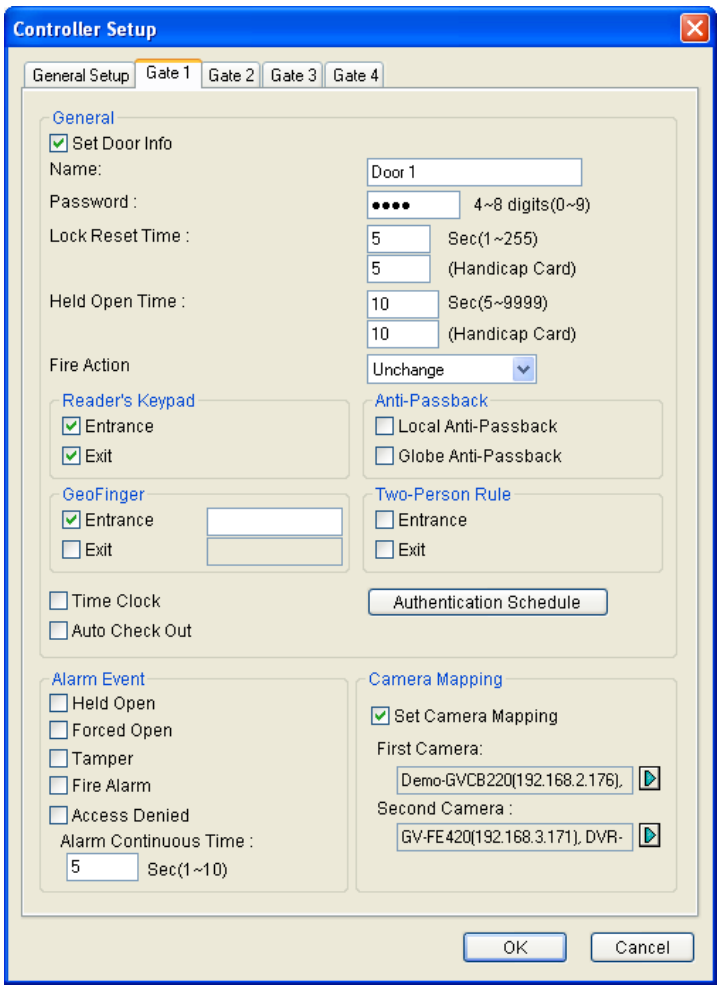


Figure 5-1

4. In the Camera Mapping section, select **Set Camera Mapping** and click the first **Arrow** button. This dialog box appears.

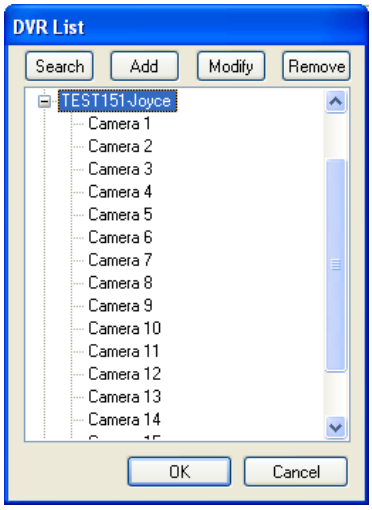


Figure 5-2

5. To connect one IP device to the GV-ASManager, use one of these ways:
   - Click **Add**, select the type of the IP device, and enter its IP address and login information.
   - Click **Search** to detect all GeoVision IP devices on the same LAN. After the found IP device is added, you must click the **Modify** button to enter its login ID and password.
6. Expand the Host folder listed in the DVR List dialog box (Figure 5-2), select one camera and click **OK**. The mapped **Host Name** and **Camera** are displayed on the Controller Setup dialog box.
7. To map the second camera to the door, click the second **Arrow** button, and follow Steps 5 and 6 to add another camera.
8. Click **OK** and return to the main screen.
9. Click the specific door on the Device View window. The associated live view is displayed on the Live Video window.

Tip:

1. You can modify the host or camera name in the DVR List dialog box (Figure 5-2) by clicking the listed name directly.
2. GV-ASManager is compatible with third-party IP devices using RTSP, ONVIF and PSIA protocols. To connect through RTSP, ONVIF and PSIA protocols, click the **Add** button, select **Add IPCam Mapping** and select **Protocol** in the **Brand** drop-down list to choose the type of protocol. For the RTSP commands, refer to the third-party IP camera's user manual.

5.2 Accessing a Live View

After mapping cameras to doors, use one of the following methods to access a live view on the Live Video window:

- On the Device View window, click the desired door. Its associated live view will appear.
- On the Camera List window, click the desired camera. Its associated live view will appear.
- On the Alarm Monitor and Access Monitor windows, click the desired event. Its associated live view will appear.

To access live views from multiple IP devices, see *5.4 The Multiview Window* below.

5.2.1 Live Video Window

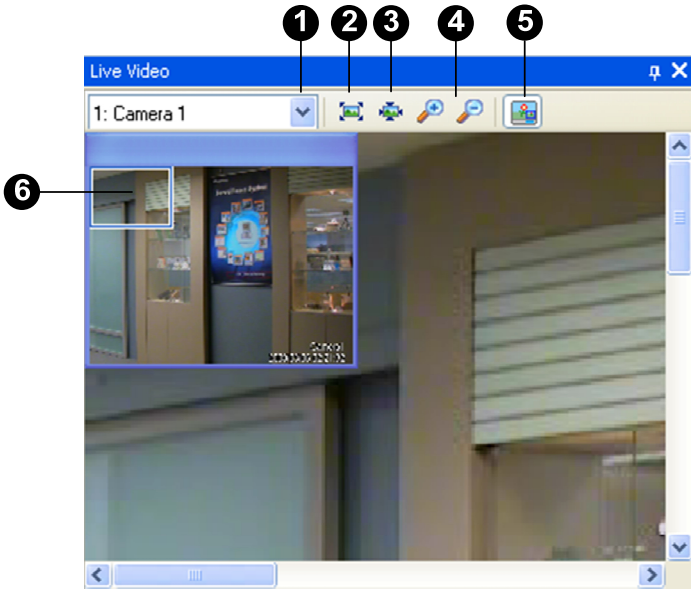


Figure 5-3

The controls on the Live Video window:

No.	Name	Function
1	Camera List	Switches between two cameras when you have mapped two cameras to the selected door.
2	Best Fit	Rescales the image to fit any resized window.
3	Actual Size	Displays the image in its original size.
4	Zoom	Zooms in or out the image.
5	Thumbnail	Displays a thumbnail view (No. 6). When the image size is larger than the Live Video window, drag the box in the thumbnail view to have a close look at the image.
6	Thumbnail View	See the description in No. 5.

5.3 Accessing a Video Image

You can access the video image captured after the access and alarm triggered event.

- On the Access Monitor or Alarm Monitor window, double-click the desired event to display the image. Or, right-click the desired event and select **Show Image** to display the image. Notice if there is no image retrievable, the option will be grayed out.

5.4 The MultiView Window

The MultiView window provides a quick view of up to sixteen preset cameras on one screen. These cameras can be a mix of cameras from several IP devices.

To open and use MultiView:

1. On the menu bar, click **View** and select **MultiView**. The MultiView window appears, similar to Figure 5-4.
2. Drag the desired camera from the Camera List window, and drop it to the required frame on MultiView.

The video generated by the camera appears in this frame. If a different camera view already exists in this frame, the new video takes its place.

Figure 5-4

The controls on the MultiView window:

No.	Name	Function
1	Frame	The frame displays live video from the assigned camera. The camera number and name, controller ID and name will be displayed in the upper left corner.
2	3D	Click this option to have a dynamic 3D live view. In the 3D live view: • Double-click one camera view to switch between 3D mode and thumbnails. Then right-click the 3D image to have different 3D effects. • Double-click one camera view in thumbnails to change different divisions (4, 9 and 16 divisions).
3	Camera List	Select the desired camera. The selected camera will be displayed with mouse focus.
4	Previous / Next Page	Go to the previous or next page of camera views.
5	Matrix View	Select an existing Matrix View (a group of views) from the drop-down list. For details, see *5.4.1 Adding a Matrix View*.
6	Add Matrix	Add a Matrix View.
7	Delete Matrix	Delete a Matrix View.
8	Resolution	Select the image resolution. Double-click one camera view to rescale the image to fit the MultiView window or restore to its set resolution.

Note: It is possible to drag the MultiView window out of the main screen and even drag the window to place at the second computer monitor.

5.4.1 Adding a Matrix View

A Matrix View, or a group of views, is a programmed arrangement of frames in the MultiView window that can present up to sixteen different camera views. Multiple Matrix Views can be added as required.

1. In the Matrix View drop-down list (No. 5, Figure 5-4), enter a name for the Matrix View.
2. Click the **Add Matrix** button. The Matrix View name is created.
3. Drag the desired camera from the Camera List window to an available frame in the window. The video associated with the camera is displayed in the frame.
4. You can repeat Steps 1-3 to add more than one Matrix View. And use the drop-down list to change to a different Matrix View.

5.5 Retrieving Recorded Video

Recorded video can be reviewed by retrieving the video from the DVR (GV-System / GV-NVR) and playing it back. Before you can review video recorded on the DVR, the following function must be enabled to allow remote access:

- DVR: Enable **Remote ViewLog Service** on Control Center Server

To play back video:

- On the Access Monitor or Alarm Monitor window, click the desired event. If recorded video exits, the Playback window will be enabled. Click the **Play** button to play the video clip.

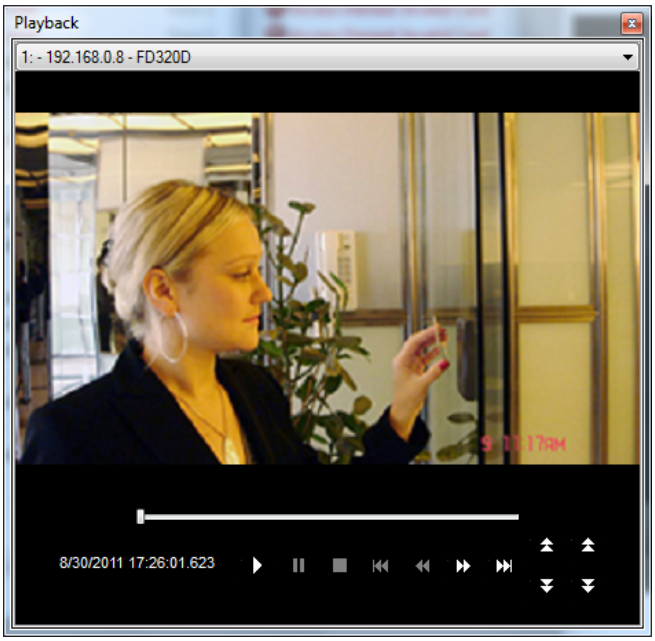


Figure 5-5

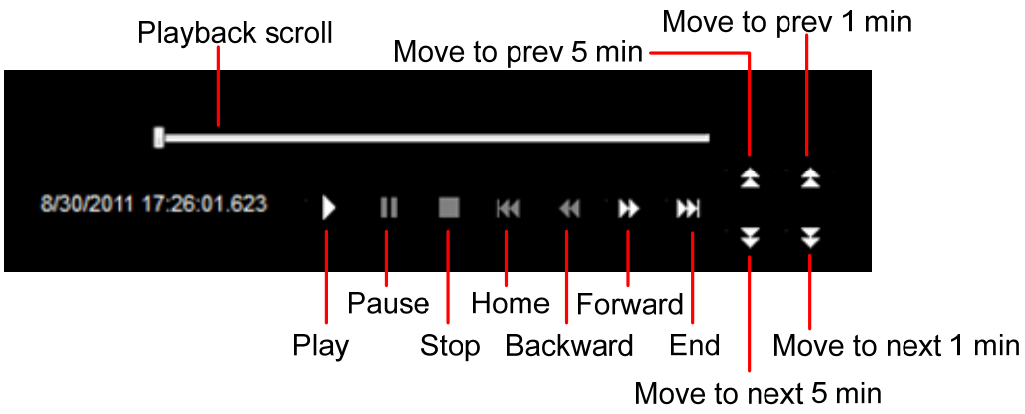


Figure 5-6

Right-click the window to have the following features:

Play Mode	Includes these options: • **Frame by Frame:** Plays back video frame by frame. • **Real Time:** Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback. • **Auto Play Next 5 Minutes:** Plays back video up to 5 minutes. • **Audio:** Turns on or off the video sound.
Render	Includes these options: • **Deinterlace:** Converts the interlaced video into non-interlaced video. • **Scaling:** Smoothens mosaic squares when enlarging a playback video. • **Deblocking:** Removes the block-like artifacts from low-quality and highly compressed video. • **Defog:** Enhances image visibility. • **Stabilizer:** Reduces camera shake. • **Text overlay's camera name and time:** Overlays camera name and time onto the video. • **Text overlay's POS/GV-Wiegand:** Overlays POS or GV-Wiegand Capture data onto the video. • **Full Screen:** Switches to the full screen view.
Tools	• **Snapshot:** Saves a video image. • **Save as AVI:** Saves a video as avi format. • **Download:** Downloads the video clip from a GeoVision IP device to the local computer.

Chapter 6 Anti-Passback

The Anti-Passback is used to ensure one-card and one-way access into and then out of a controlled area. This function prevents card holders from passing their cards back to a second person to gain entry into the same controlled area. Depending on the number of controllers and communication link, there are three types of Anti-Passback operations: **Anti-Passback**, **Local Anti-Passback** and **Global Anti-Passback**.

Anti-Passback is performed only on one controller, while Local Anti-Passback and Global Anti-Passback can be performed on multiple controllers. Anti-Passback is performed through either RS-485 or TCP/IP connection, while Local Anti-Passback and Global Anti-Passback are performed only through TCP/IP connection. The following table lists the supported operations among GV-AS Controllers.

Model	Anti-Passback	Local Anti-Passback	Global Anti-Passback
GV-AS100	Yes	Yes (GV-ASBox or GV-ASNet required)	Yes (GV-ASBox or GV-ASNet required)
GV-AS110	Yes	Yes (GV-ASBox or GV-ASNet required)	Yes (GV-ASBox or GV-ASNet required)
GV-AS120	Yes	Yes (GV-ASBox or GV-ASNet required)	Yes (GV-ASBox or GV-ASNet required)
GV-AS400	Yes	Yes	Yes

6.1 Anti-Passback

Anti-Passback is used on **one controller only**. For this application, select **Local Anti-Passback** at the **Gate** tab of the Controller Setup dialog box (Figure 4-3).

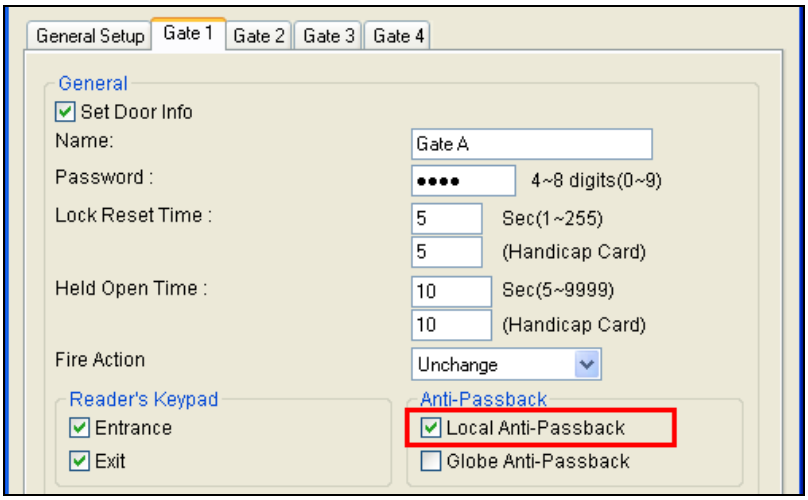


Figure 6-1

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

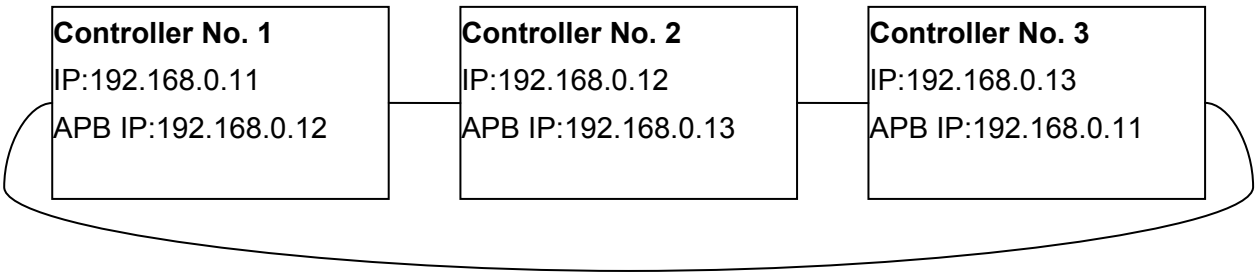
6.2 Local Anti-Passback

Local Anti-Passback is used on **multiple controllers which are associated with network connections**. Before you start, the following conditions must be true:

- The communication mode between GV-ASManager and GV-AS Controller is Ethernet.
- LAN environment is applied.

Here we use three **GV-AS400 Controllers** as example to explain how to combine three controllers together to operate the Anti-Passback (APB) function. Since Anti-Passback is performed in a network connection, every controller has a unique IP address. When three controllers are connected for Anti-Passback, an APB IP address is then applied for interaction.

For example, Controller No. 1, No. 2 and No. 3 are combined in sequence, as illustrated below. APB IP is the IP address of the associated controller.
IP of Controller No. 1 is 192.168.0.11; APB IP of Controller No. 1 is IP of Controller No. 2.
IP of Controller No. 2 is 192.168.0.12; APB IP of Controller No. 2 is IP of Controller No. 3.
IP of Controller No. 3 is 192.168.0.13; APB IP of Controller No. 3 is IP of Controller No. 1.



To configure Anti-Passback for the three GV-AS400 Controllers:

1. Access the **AS400 Setting** page of the Controller No. 1 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 2, e.g. 192.168.0.12.

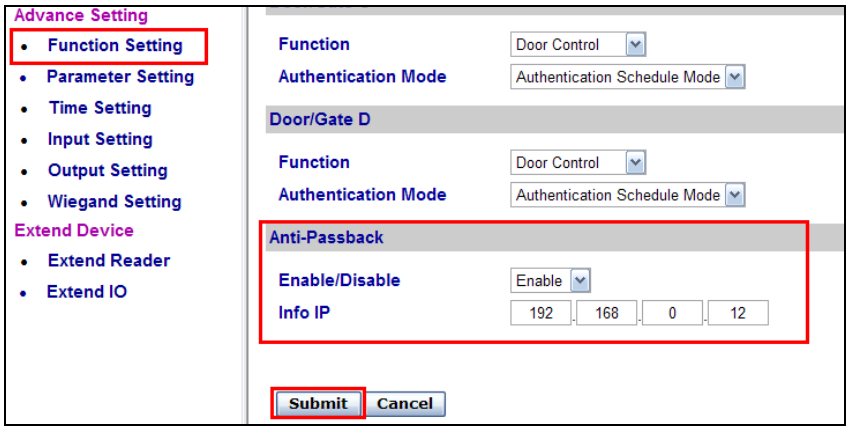


Figure 6-2

2. Access the **AS400 Setting** page of the Controller No. 2 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 3, e.g. 192.168.0.13.
3. Access the **AS400 Setting** page of the Controller No. 3 Web interface. In the Anti-Passback section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 1, e.g. 192.168.0.11.
4. On the ASManager, select **Local Anti-Passback** (Figure 6-1) to start the function.

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

6.3 Global Anti-Passback

Global Anti-Passback can not only prevent the use of a card to gain successive entries, but track the card holder around the site.

The diagram below shows a typical site controlled by access control. The following sections will guide you through the steps you would need to go through to configure this site for Global Anti-Passback.

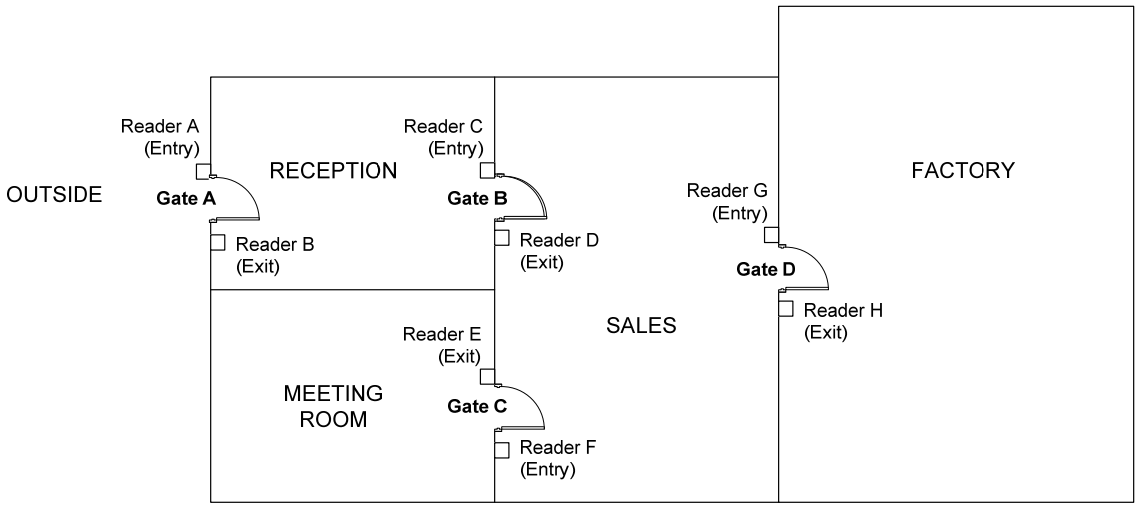


Figure 6-3

6.3.1 Step 1: Enabling Global Anti-Passback

Select **Global Anti-Passback** at each **Gate** tab of the Controller Setup dialog box (Figure 4-3).

6.3.2 Step 2: Configuring Areas

This step is to define the Entry and Exit areas for each door/gate and name the areas properly.

- On the menu bar, click **Setup** and select **Areas**. This dialog box appears.

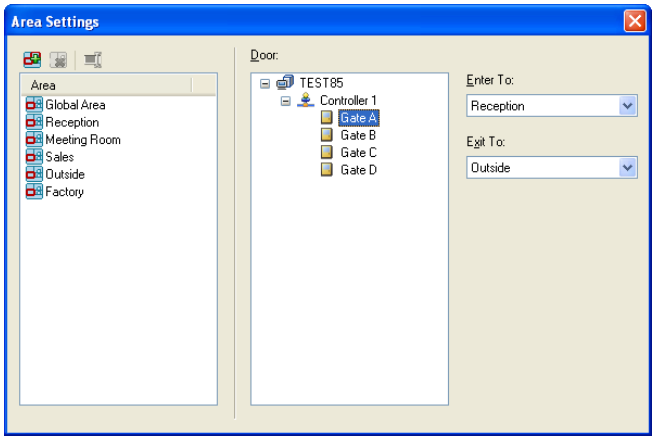


Figure 6-4

Enter to is the area where you enter by accessing the Entry reader. **Exit to** is the area where you exit to by accessing the Exit reader. In this case, we set up like this:
Gate A: **Enter to** Reception; **Exit to** Outside
Gate B: **Enter to** Sales; **Exit to** Reception
Gate C: **Enter to** Meeting Room; **Exit to** Sales
Gate D: **Enter to** Factory; **Exit to** Sales

6.3.3 Step 3: Configuring Readers

This step is to define the Entry and Exit readers for each door/gate. The reader definition tells the GV-ASManager which reader controls the access across the area boundaries.

When card holders access the unauthorized readers, the message **Access Denied: APB (Wrong Area)** will be displayed and the door will remain locked. When card holders access the same reader successively, the message **Access Denied: APB (Double Entry)** will be displayed and the door will remain locked.

To define readers, you can use GV-ASKeypad or the Web interface of the GV-AS Controller. Here we use the GV-AS400 Web interface as example to define Wiegand readers. For this case, Wiegand reader A (Entry) goes from Outside to Reception, Wiegand reader B (Exit) goes from Reception to Outside and etc.

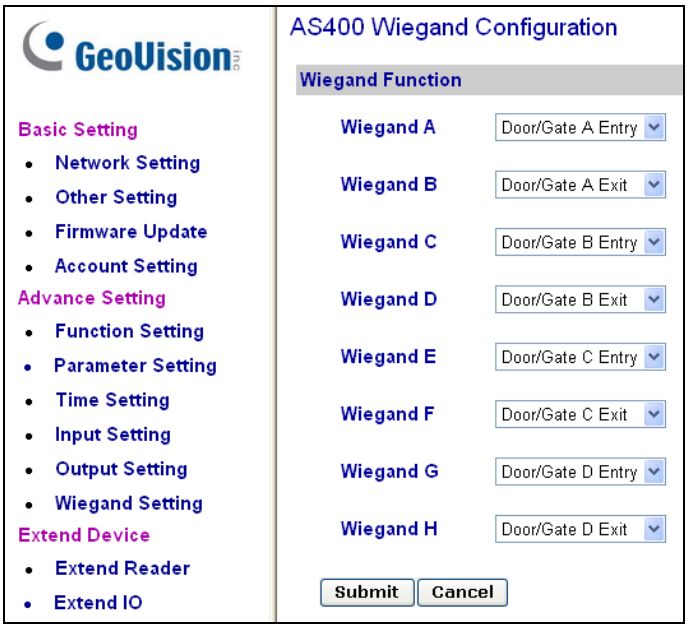


Figure 6-5

6.3.4 Step 4: Configuring Door Contacts

This step is to define the door contact sensor for each door/gate. When the door contact sensor is triggered and the door is unlocked, the GV-ASManager can tell where a card holder is based on your area definition at Step 1.

To define door contact sensors, you need to use the Web interface of GV-AS Controller. In this example of GV-AS400 Web interface, Input 01 is used as Door Contact of Door A, Input 02 is used as Door Contact of Door B and etc.

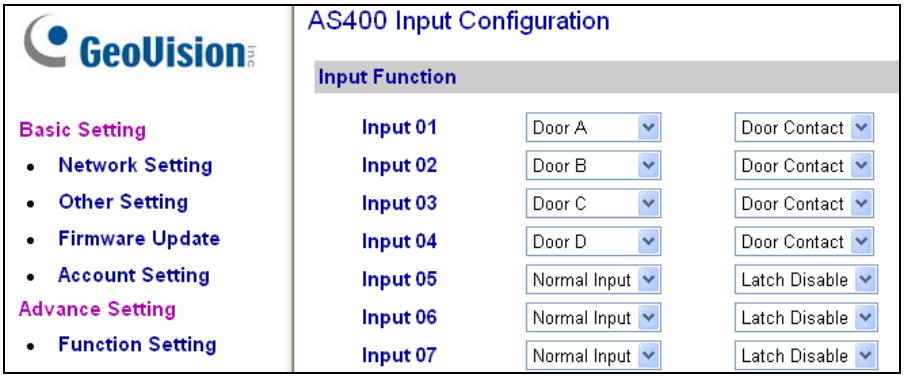


Figure 6-6

6.3.5 Step 5: Locating Card Holders

To locate a card holder, select **Monitoring** on the menu bar and select **New Locate Person**. When the Exit or Entry reader is triggered, the GV-ASManager can tell if card holders follow Anti-Passback rules and then grand or deny the access. When the door contact sensor is triggered, the GV-ASManager can tell the location where the card holder is now.

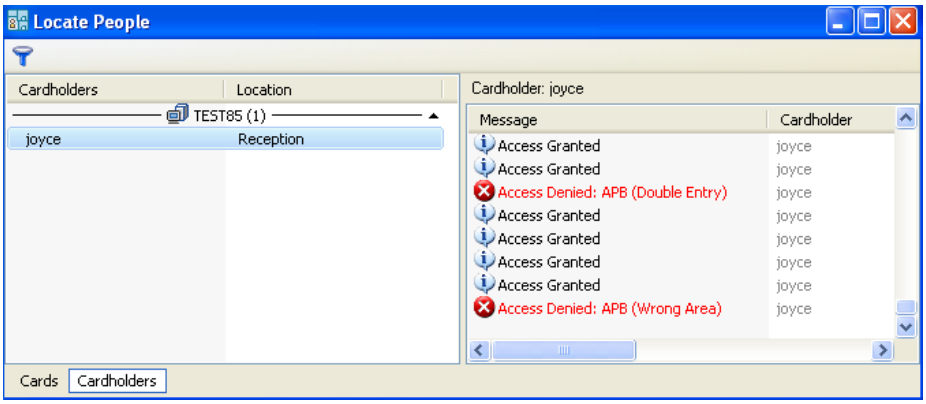


Figure 6-7

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View window (Figure 3-3) and select **Reset Anti-Passback**.

Chapter 7 Other Functions

7.1 System User Setup

A system user is a person using the GV-ASManager to monitor door controllers, enroll cardholders or program the system. Using this function, the system supervisor can create new system users with different access rights. Up to 1,000 user accounts can be created.

7.1.1 Adding a New User

1. On the menu bar, click **Tools** and select **Operators**. This dialog box appears.

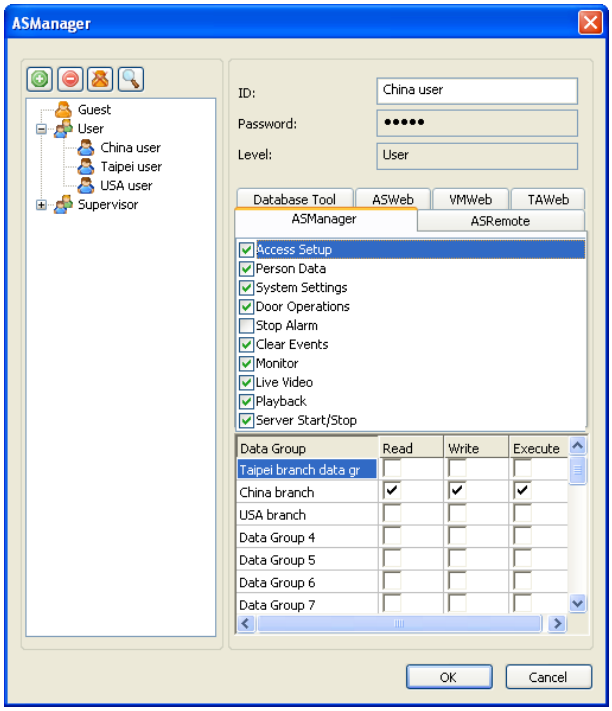


Figure 7-1

2. Click the **New** button at the top left corner. This dialog box appears.

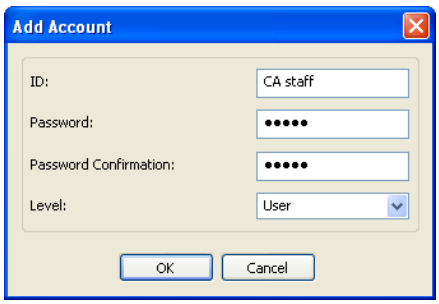


Figure 7-2

3. Type the user's **ID** and **Password**. Re-enter the same password in the Password Confirmation field.
4. Give a **Hint** (optional) that would remind you of the password.
5. Set the user's authorization level to **Supervisor** or **User**. By default, users belonging to the Supervisor level have full rights and permissions to system settings. Users belonging to the User level are restricted from all system settings, and have only limited access to certain functions.
6. Click **OK** to add the user.
7. Click the tab **ASManager**, **ASRemote**, **ASWeb**, **Database Tool**, **VMWeb** or **TAWeb** in the middle of the window. Select the functions to grant access to the system user.
8. In the **Data Group** section, you can optionally select a data group and specify whether the user account will be able to read, write and execute the functions assigned under the data group. A data group may include controllers, cards, cardholders, access groups, time zones and weekly schedules. Up to 32 data groups can be created. You can click the name of the data group to type a different name.
   - **Read:** Privilege to view settings.
   - **Write:** Privilege to view and change settings. When Write is selected, Read will automatically be selected.
   - **Execute:** Privilege to open door, close door and turn off alarm.

   For example, if you select Data Group 4 and only select **Write**, the user will be able to view and change only the settings of the controllers, cards, cardholders, access groups, time zones and weekly schedules assigned under Data Group 4.

7.1.2 Editing an Exiting User

Only supervisors are allowed to edit the information of a system user.

1. Select a user from the user list to display its properties. Or, right-click on a user level (User or Supervisor), and then select **Find Specific Account** for a quick search. A valid password is required to edit a supervisor.
2. Edit the properties as required. Check the **Account Is Disabled** option if you wish to disable this user.

7.2 Notification Setup

When alarm conditions occur the system can automatically send SMS alerts and e-mail alerts to one or multiple recipients, as well as activating computer alarm.

7.2.1 Setting SMS Server

Before you can send out SMS alerts, you should configure the SMS server.

1. On the menu bar, click **Tools** and select **SMS Server Settings**. This dialog box appears.

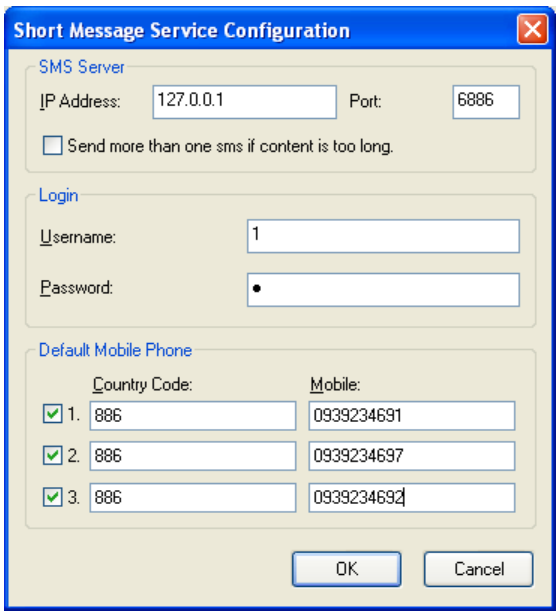


Figure 7-3

2. Type the IP address of the SMS server, its login username and password. Then assign up to three mobile numbers, including country code, which SMS alerts should be sent to. Click **OK**.
3. To enable the SMS connection, click **Tools** on the menu bar and select **Connect to SMS Server**.

Note: For ASCII encoding (English language), SMS text messages are limited to 160 characters; for Unicode encoding (other languages), SMS text messages are limited to 70 characters. If you want to send longer text messages, select **Send more than one sms if content is too long.** The long messages will be split up to 9 segments and go out as multiple SMS messages.

7.2.2 Setting E-Mail Server

Before you can send out e-mail alerts, you should configure the e-mail server.

1. On the menu bar, click **Tools** and select **Email Server Settings**. This dialog box appears.

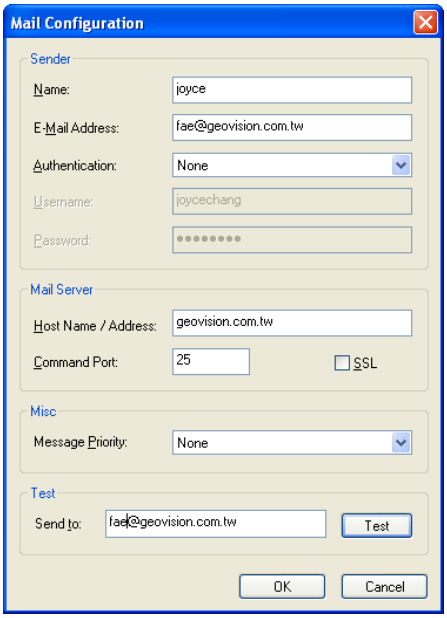


Figure 7-4

2. Set up the following options:

   - **Name:** Type the sender's name.
   - **E-Mail Address:** Type the sender's e-mail address.
   - **Authentication:** If your mail server requires authentication for sending e-mails, select one type of authentication, and type the valid username and password.
   - **Host Name/Address:** Type the name of the mail server.
   - **Command Port:** Keep the default port 25, or modify it to match that of the mail server.
   - **SSL:** Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of Internet connection. When the option is enabled, the Command Port is changed to 465.
   - **Message Priority:** Assign the message a priority so the recipient knows to either look at it right away (high priority) or read it when time permits (low priority). A high priority message has an exclamation point next to it. Low priority is indicated by a down arrow.
   - **Send to:** Type a valid e-mail address and click the **Test** button to check if the server setup is correctly configured.

7.2.3 Setting Notification

1. On the menu bar, click **Tools** and select **Notifications**. This dialog box appears.

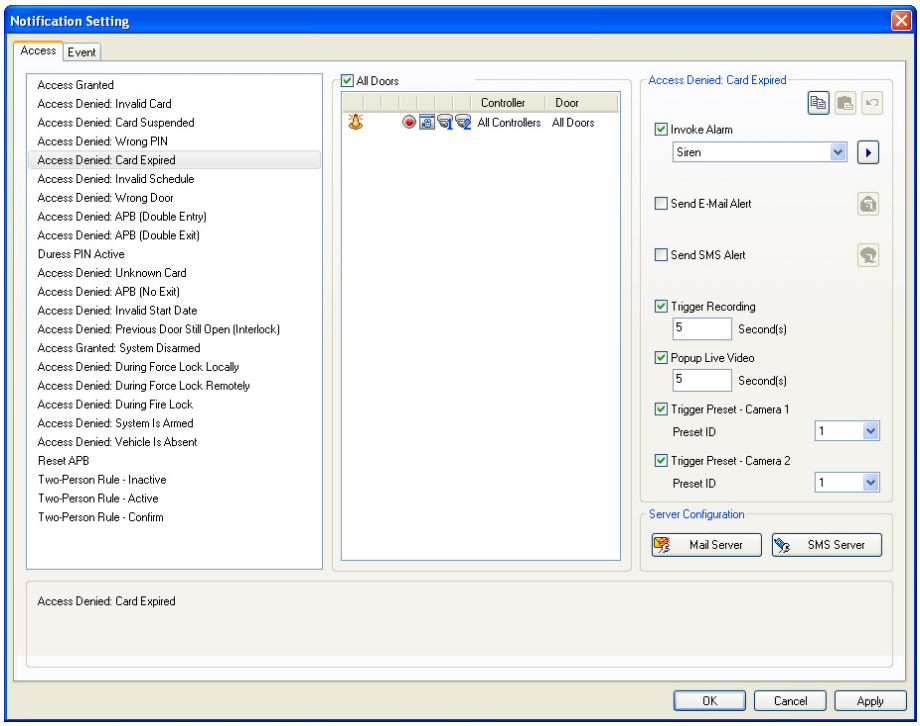


Figure 7-5

2. Use the **Access** and **Event** tabs to select a desired event for configuring alert methods.
3. Define the following alert approaches:

   - **Invoke Alarm:** Enable the computer alarm when the selected event occurs.
   - **Send E-Mail Alert:** When you select this option, an e-mail will pop up. Enter the recipient's e-mail address and alert subject. Then you can enter your own content, or use the buttons on the text window to send out the programmed information automatically.

     For example, if you click the button, the sent SMS alert will include the controller information. For details see *C. E-Mail and SMS Alert Symbols* in *Appendix*.
   - **Send SMS Alert:** When you select this option, a dialog box will pop up. Ensure the preset mobile number(s). Select Text Code Type. Then type your messages; otherwise click the buttons on the text window to send out the programmed information automatically. See the above example in "Send E-Mail Alert".
   - **Trigger Recording:** Enable recording of DVR, Video Server or Compact DVR when the selected event occurs. You can specify the recording time between 1 and 300 seconds. For the function to work, you must activate monitoring on these IP devices ahead.

- **Popup Live View:** An associated live view will pop up for alert when the selected event occurs. You can specify the duration of the live view remains on the screen between 1 and 300 seconds.
- **Trigger Preset:** Direct the camera(s) to a preset point when the selected event occurs.

4. To define more than one event with the same alert configuration, first right-click the previously defined event on the list and select **Copy** to save its settings. Then use Ctrl + left click or Shift + left click to select several events. Right-click the selected events and select **Paste** to have the same settings.

Note: For text code type, select **ASCII** for English that is limited to 160 characters and select **Unicode** for text of other languages that is limited to 70 characters.

7.3 Startup and Backup Setup

You can select which server should be enabled upon Windows or GV-ASManager startup.

You can also specify a path for the **Auto Backup** function to automatically save another copy of log and image files. The Auto Backup function performs backup at 24:00 A.M every day. By default, the log and image files are saved at **C:\Access Control\ASManager\ASBackup**.

- To access these functions, click **Tools** on the menu bar and select **Option**.

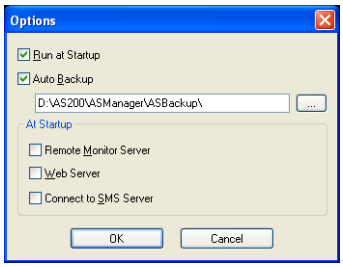


Figure 7-6

Note: To back up the Configuration files, see *12.3 Other Database Settings*.

7.4 Enrolling Fingerprints

GV-ASManager can work with **GV-GF 1901** reader to enroll cardholders' fingerprints and transmit the fingerprint data to **GV-GF 1901/1902** readers installed on GV-AS Controllers. To gain access the cardholder must present the enrolled fingerprint.

The wiring for this application is illustrated as below. GV-GF 1901 reader installed on GV-ASManager is only for enrolling fingerprints. GV-GF 1901/1902 readers installed on GV-AS Controllers receive the fingerprint data from GV-ASManager and verify the present fingerprint.

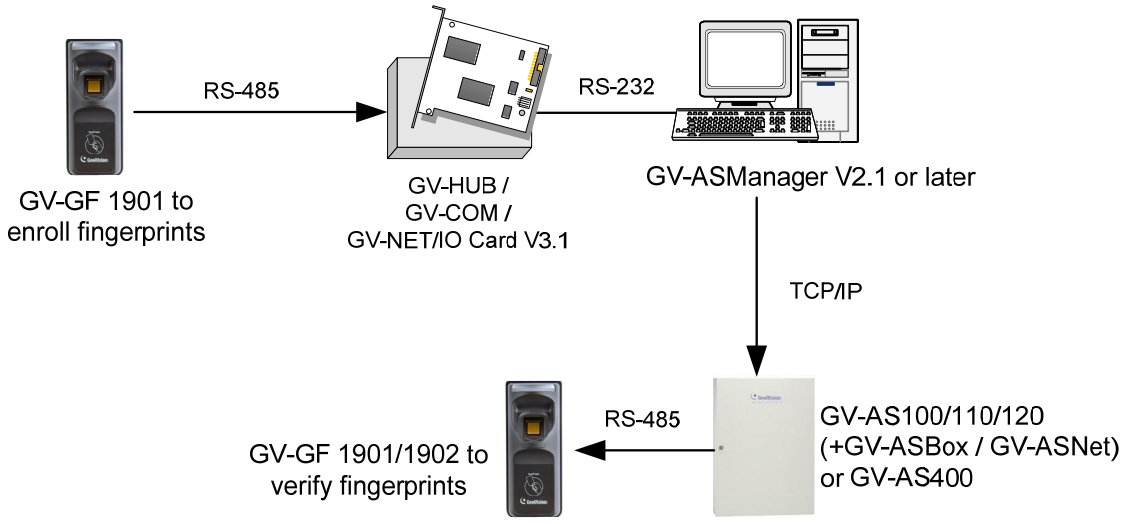


Figure 7-7

Note: The fingerprint enrollment does not support the Wiegand connection.

7.4.1 Connecting to GV-GF Fingerprint Readers

The communication link between GV-GF Fingerprint Readers and the computer running GV-ASManager must be RS-485. For the RS-485 connection to the computer, a RS-485 to RS-232 converter, such as GV-COM, GV-Hub or GV-NET/IO Card, is required. Refer to Figure 7-7.

7.4.2 Enrolling Fingerprints

Before you start, you have to complete the card and cardholder enrollments. See *4.3 Setting Cards* and *4.6 Setting Cardholders.*

Note: If your GV-AS Controller is not equipped with any card readers, it is still required to enroll cards because each fingerprint needs to go along with a card number. In this case, you can create virtual card numbers to represent the enrolled fingerprints.

To enroll fingerprints:

1. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List window appears.
2. Double-click one cardholder listed in the window. The Cardholder Setup dialog box appears.
3. Click the **Fingerprint** tab. This dialog box appears.

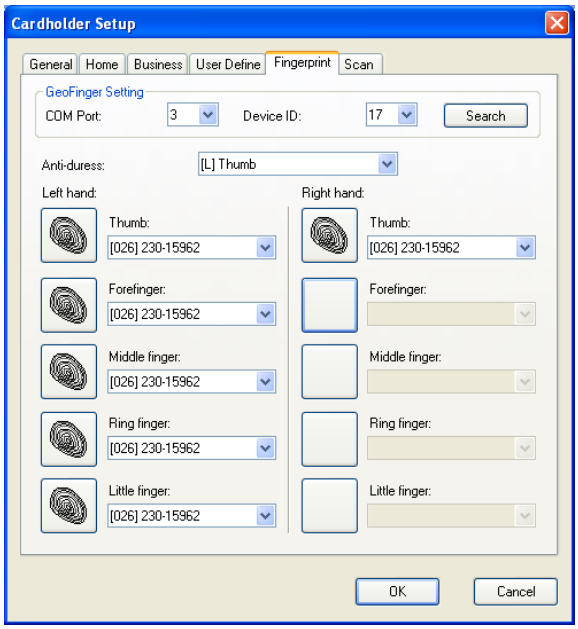


Figure 7-8

4. Click the **Search** button to detect the GV-GF Fingerprint Readers connected.
5. In the Left Hand and Right Hand sections, click any finger square to enroll the fingerprint.
6. Place the specific finger on the GV-GF Fingerprint Reader. It is required to register the same fingerprint twice to complete the enrollment. All ten fingerprints of a cardholder can be enrolled.
7. Use the drop-down list to assign a card to the fingerprint.

8. To delete the enrolled fingerprint, place the mouse pointer on the desired fingerprint image. The button appears. Click the button to delete the fingerprint.
9. For the **Anti-duress** function, select a fingerprint from the Anti-duress drop-down list. When the cardholder is forced to open the door under threat, he can present the designated finger to activate an alarm and send a warning signal to the GV-ASManager.
10. Click **OK** to apply the settings.

7.4.3 Uploading Fingerprints to Controllers

You can upload fingerprints to any Door/Gate installed with **GV-GF 1901/1902** readers for access control. Each GV-GF Fingerprint Reader can store up to **1,900** fingerprints.

1. Ensure the GV-GF Fingerprint Reader has been set up on the GV-AS Controller. When the GV-GF Fingerprint Reader is detected on the GV-AS Controller, a green mark should appear in the **Setting Status** field on the GV-AS Controller's Web interface. See *GV-AS Controller Installation Guide*.

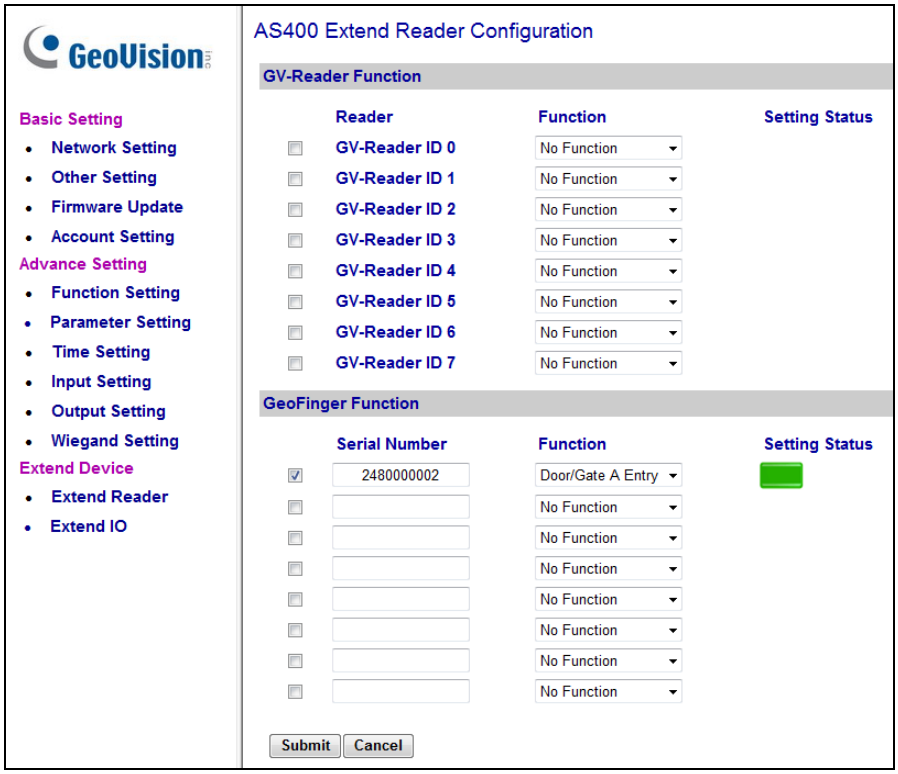


Figure 7-9

2. On the menu barr, click **Setup** and select **Fingerprint Access**. This dialog box appears.

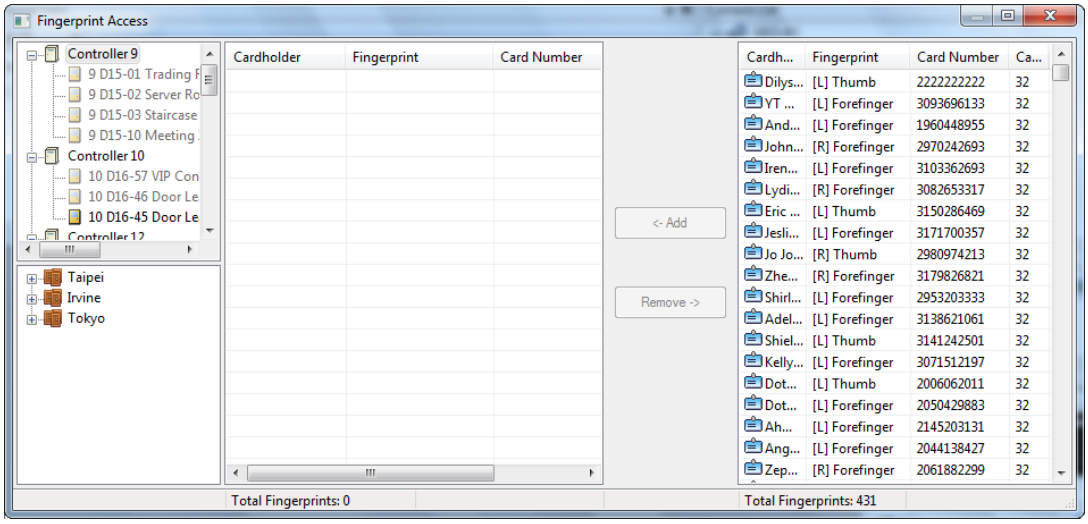


Figure 7-10

3. To upload the fingerprints to a door or a controller, select the desired Door/Gate or controller in the top-left panel. If you have assigned multiple controllers to a door group, select the desired door group in the bottom-left panel. Refer to *Uploading Fingerprints to Controllers Using Door Groups* later in this chapter to see how to set up door groups.
4. Select the desired fingerprint data on the right side. The **Add** button becomes available.
5. Click the **Add** button to upload the selected fingerprint data to the selected Door/Gate or door group. When the uploading is complete, check marks will appear in the **In** (Enter) or **Out** (Exit) columns. The resulting window after uploading may look like this:

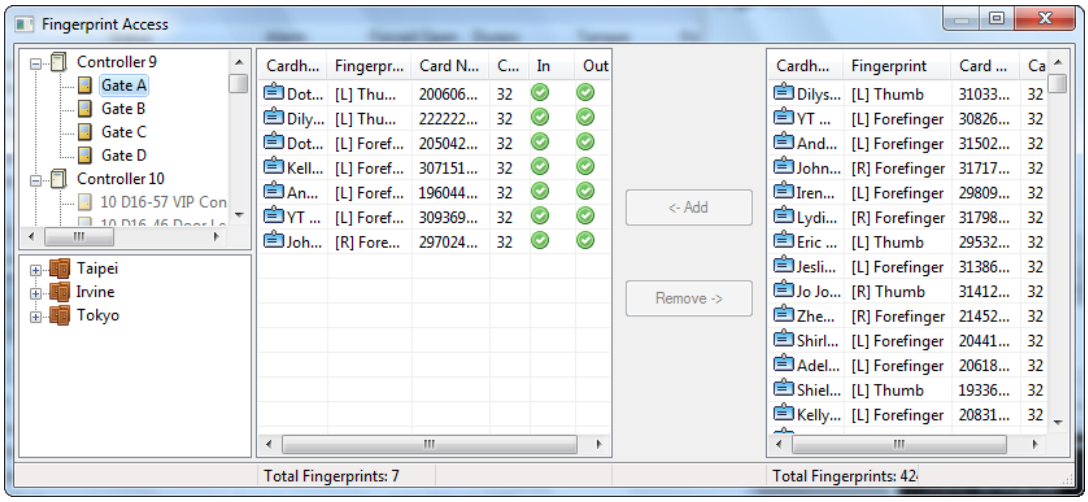


Figure 7-11

Tip: If some green checkmarks are missing in the **In** or **Out** columns, right-click the door / gate in the Device View and select **Sync GeoFinger** to re-upload the data.

7.4.4 Uploading Fingerprints to Controllers Using Door Groups

When a large number of GV-AS Controllers are connected to the GV-ASManager, you can organize the controllers into different door groups. Using door groups, you can quickly upload fingerprints to all the controllers in a door group instead of uploading to each controller one by one.

1. On the menu bar, click **Setup** and select **Door groups**. This window appears and the connected controllers are listed on the right.

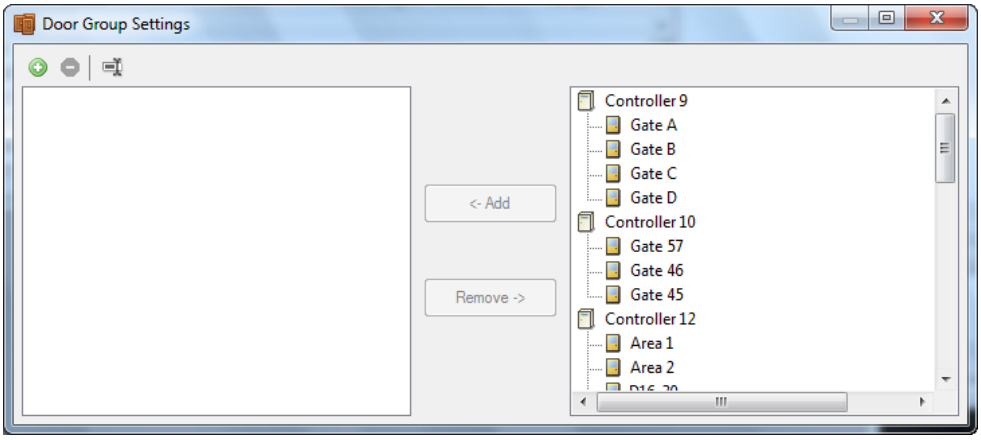


Figure 7-12

2. Click the **Add Group** button . A new group is created.
3. Click the new group and click the **Rename Group** button to rename the group.
4. Select the door group and then select the controllers to add to the group.
5. Click the **Add** button. The selected controllers are now assigned to the group.

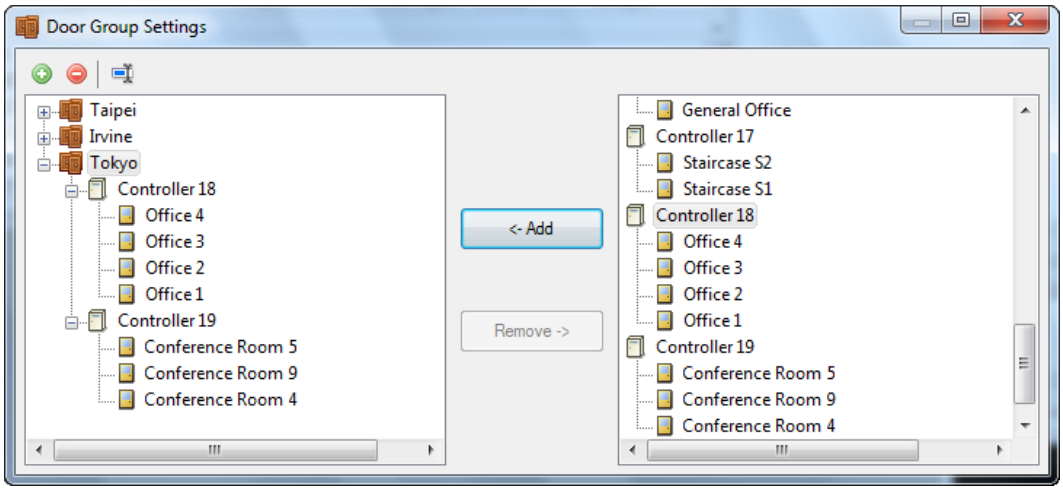


Figure 7-13

7.5 Scanning Driver's Licenses and Business Card

GV-ASManager can work with **SnapShell ID Scanner** to let you acquire and edit the personal data from driver's licenses and business cards.

Note: This function only supports SnapShell ID Scanner with SDK driver version.

---

1. Consult the Scanner's documentation to connect the Scanner with the GV-ASManager.
2. On the menu bar, click **Personnel** and select **Cardholders**. The Cardholder List dialog box appears.
3. Click the **New** button. The Cardholder Setup dialog box appears.
4. Click the **Scan** tab. This dialog box appears.

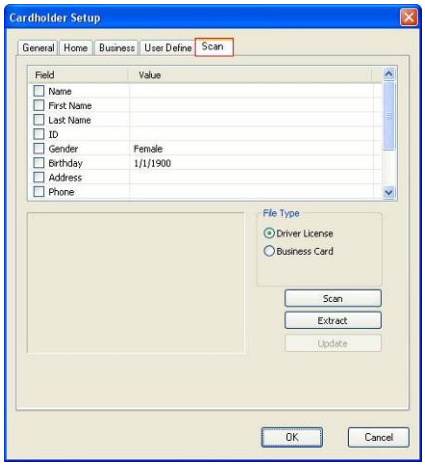


Figure 7-14

5. In the File Type field, select **Driver License** or **Business Card**. Here we use the Driver License as the example to demonstrate the following steps.

6. Place a driver's license on the Scanner and click the **Scan** button. The license image is displayed.

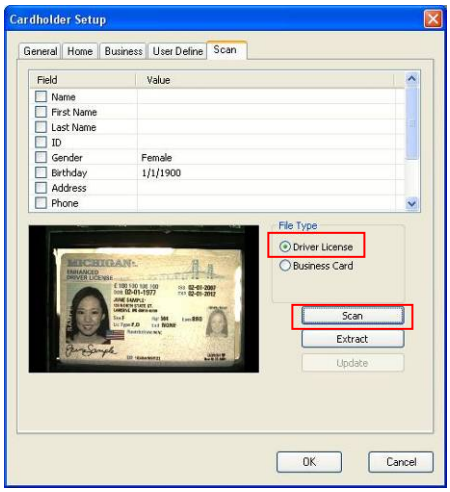


Figure 7-15

7. Click the **Extract** button to read the license data. The data is displayed in the **Value** column.
8. To modify the data, click the desired **Value** column and type the next texts. Click anywhere in the dialog box when you are finished with the modification.

Figure 7-16

9. Click the **Update** button. The data of this driver's license is saved to the GV-ASManager's database.
10. Now you can click the **Home** tab to view the information of the driver's license, or click the **Business** tab to view the information of the business card if scanned.

Chapter 8 GV-ASRemote

The client software GV-ASRemote is designed to monitor multiple GV-ASManagers over the network. The GV-ASRemote provides the following features:

- Remote monitoring
- Remote live view and playback
- Remote control: stop alarms and force the door to lock/unlock

8.1 Installing GV-ASRemote

Insert Software CD to your computer and a window will pop up automatically. Select **Install GeoVision V3.0 Access Control System**, click **GeoVision Access Control System** and follow on-screen instructions to complete the installation.

8.2 The GV-ASRemote Window

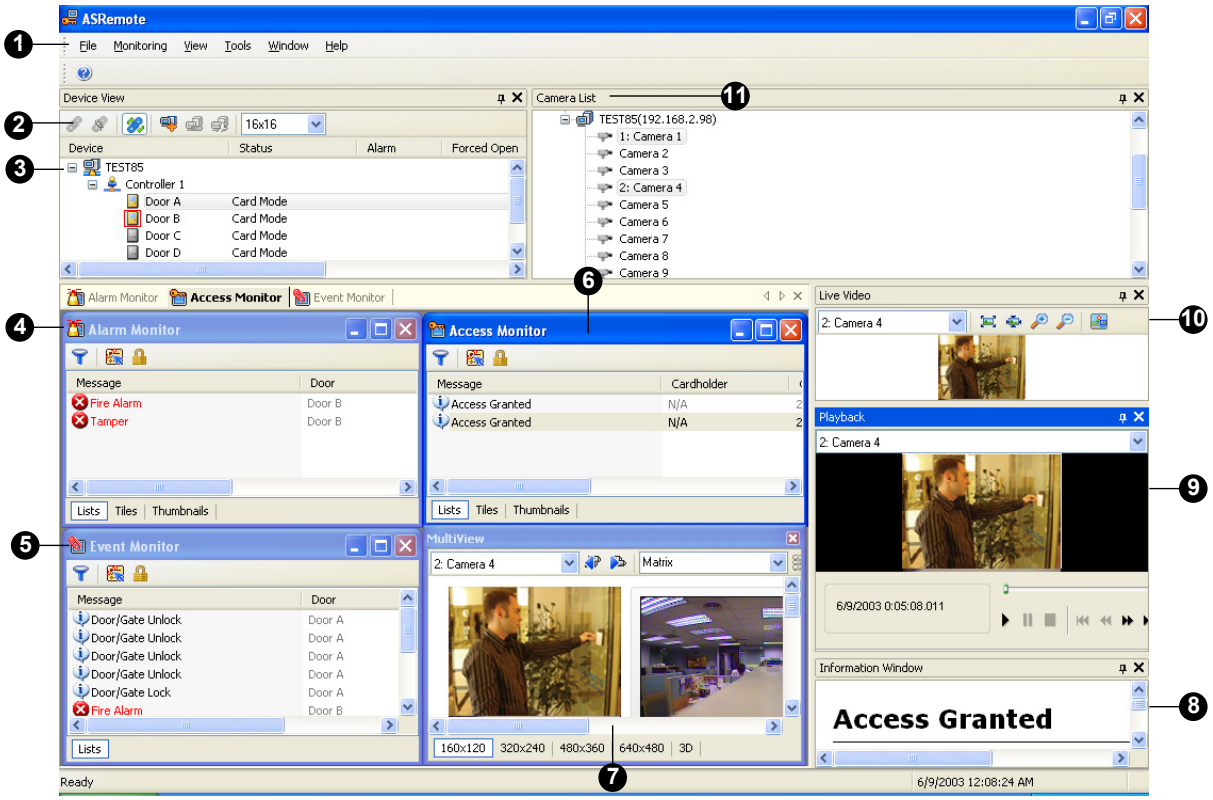


Figure 8-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of **File** (log in / out the GV-ASManager), **Monitoring** (display monitor windows of alarm, access and event), **View** (display the function windows) and **Window** (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of **Connect**, **Disconnect**, **Auto Connect**, **Add Host**, **Remove Host**, **Settings** and **Resolution**.
3	Device View	Displays a list of connected doors and their current status.
4	Alarm Monitor	Displays alarm events of doors.
5	Event Monitor	Displays monitored events of doors.
6	Access Monitor	Displays access activities of doors.
7	MultiView	Displays live views of connected cameras from multiple IP devices. For details, see *5.4 The MultiView Window*.
8	Information Window	Displays the information of doors, card readers and monitored events.
9	Playback	Plays back recorded events from a compatible GeoVision IP device. For details, see the same operations in *5.5 Retrieving Recorded Video*.
10	Live Video	Displays live views of one connected camera. For details, see the same operations in *5.2 Accessing Live View*.
11	Camera List	Displays a list of connected cameras.

8.2.1 Toolbar

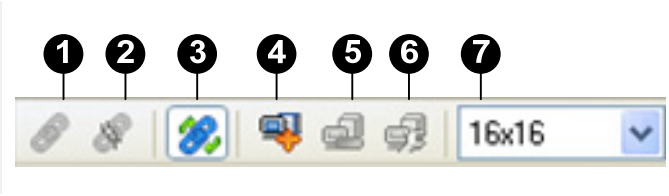


Figure 8-2

The buttons on the Toolbar of GV-ASRemote:

No.	Name	Function
1	Connect	Starts the connection with the GV-ASManager.
2	Disconnect	Ends the connection with the GV-ASManager.
3	Auto Connect	Retries to build the connection with the GV-ASManager.
4	Add Host	Adds a GV-ASManager host to the list.
5	Remove Host	Deletes a GV-ASManager host on the list.
6	Settings	Edits the settings of GV-ASManager hosts.
7	Resolution	Changes the size of icons to 16 x 16, 24 x 24 or 32 x 32.

8.3 Connecting to GV-ASManager

Before GV-ASRemote may connect to one GV-ASManager, the GV-ASManager must allow the remote access by this procedure:

- Click **Tools** on the menu bar, select **Servers** and enable **Remote Monitor Server**.

  When the server is started, the icon appears at the bottom of the main screen.

To create a GV-ASManager host and enable connection to the GV-ASManager:

1. On the toolbar, click the **Add Host** button. This dialog box appears.

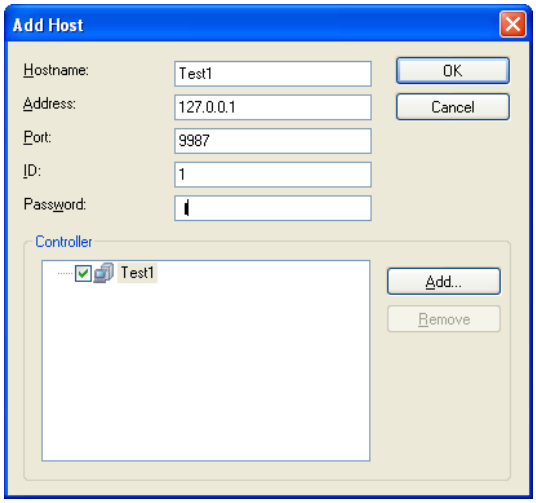


Figure 8-3

2. Give a hostname, type the GV-ASManager's IP address, modify the port number if necessary, and type the GV-ASManager's login ID and password.
3. Click **Add**. This dialog box appears.

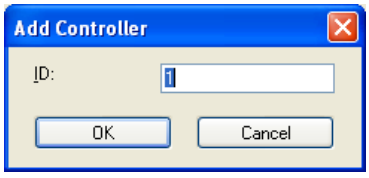


Figure 8-4

4. Type the ID of the controller associated with the GV-ASManager and click **OK.**
5. To add more controllers, repeat Steps 3-4.

6. Click **OK** and return to the main screen. A host folder will be displayed on the Device View window as example below.

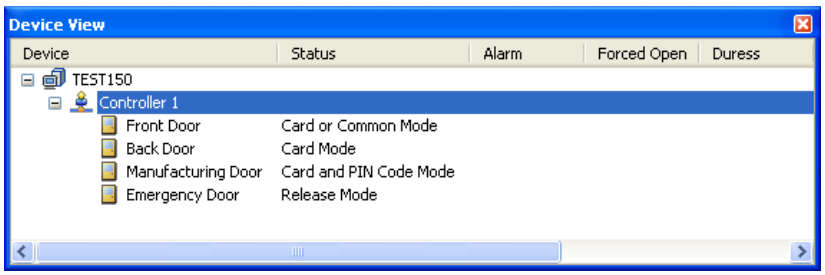


Figure 8-5

If the icon appears, it indicates the connection between GV-ASManager and GV-ASRemote has been established.

If the icon appears, it indicates the connection failed. Make sure GV-ASManager is enabled for the Remote Monitor Server function.

Note: For the disconnection messages displayed on the Status column (Figure 4-5), see *D. Controller Status* in Appendix.

Chapter 9 GV-ASWeb

The GV-ASWeb allows you to access data and settings on the GV-ASManager over the Internet. Connecting to one GV-ASManager at a time, users can remotely view event data, download logs in different formats, and set up camera / cards / cardholders / controllers / schedule using Web interface.

To use the GV-ASWeb, the version of browser in the client PC must be **Internet Explorer 7 or later**.

9.1 Connecting to GV-ASManager

Before GV-ASWeb can connect to a GV-ASManager, the GV-ASManager must be set to allow remote access:

- On the menu bar, click **Tools**, select **Servers** and enable **Web Server**. This dialog box appears.

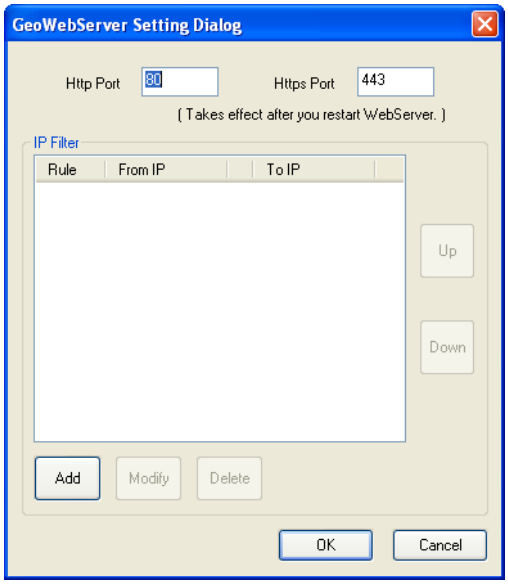


Figure 9-1

If you want to grant or deny the access from certain IP addresses, click **Add**, and type the IP addresses. Otherwise click **OK** to start the connection. When the server is started, the icon appears at the bottom of the main screen.

To start the GV-ASWeb:

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected. This web page appears.

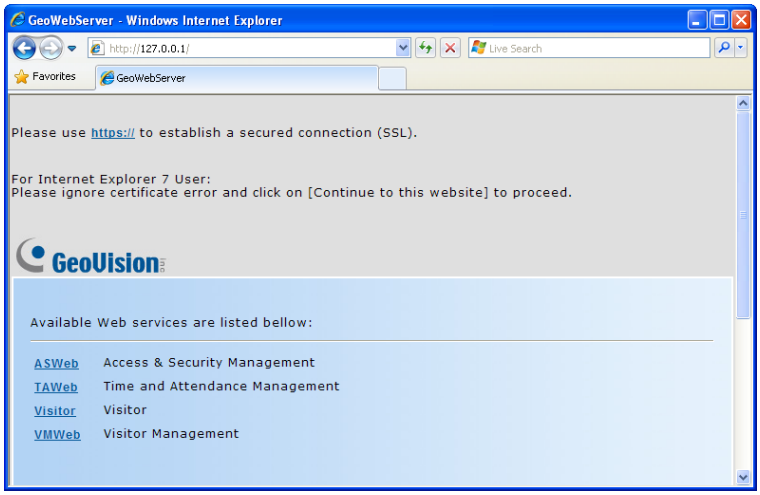

GeoWebServer - Windows Internet Explorer
http://127.0.0.1/
Favorites
GeoWebServer
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb Access & Security Management
TAWeb Time and Attendance Management
Visitor Visitor
VMWeb Visitor Management

Figure 9-2

2. Click **https://** for SSL encrypted connection, or **ASWeb** for regular connection.
3. Enter a valid username and password for login. The GV-ASWeb page appears.

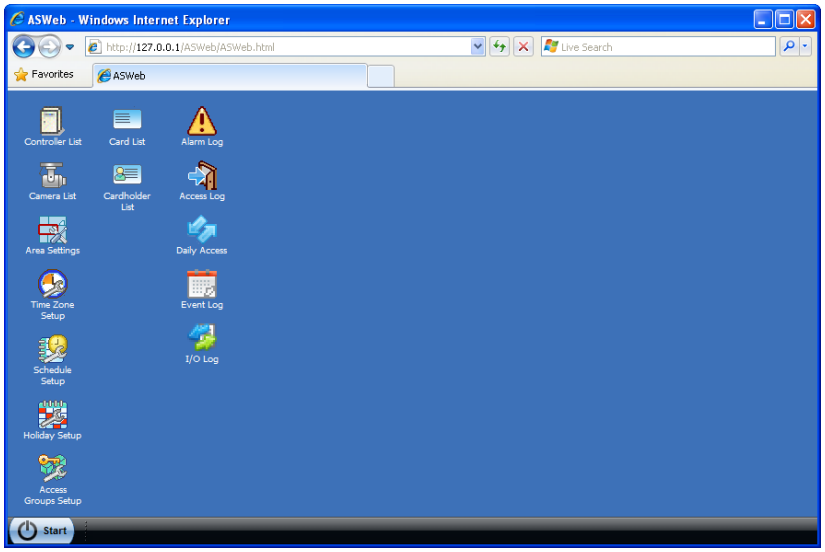


Figure 9-3

9.2 Accessing Logs

You can access the logs of the connected GV-ASManager, including Access Log, Daily Access, Alarm Log, Event Log and I/O Log. In addition, you can set up search criteria to view the records more efficiently.

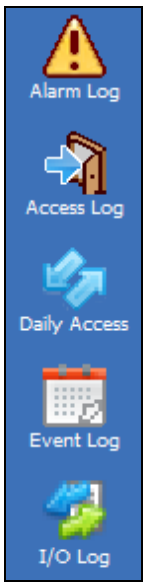


Figure 9-4

9.2.1 Setting Search Criteria

1. Select a log you want to view. Here we use Access Log as an example.
2. In the Filter section on the left, type or select the desired filtering criteria. For example, we want to search the log for the records that match the conditions of “Access Granted”, Card Number “120-38620”, Gate A entrance of AS400, and dates from November 21st to November 27th. The resulting filter window may look like this.

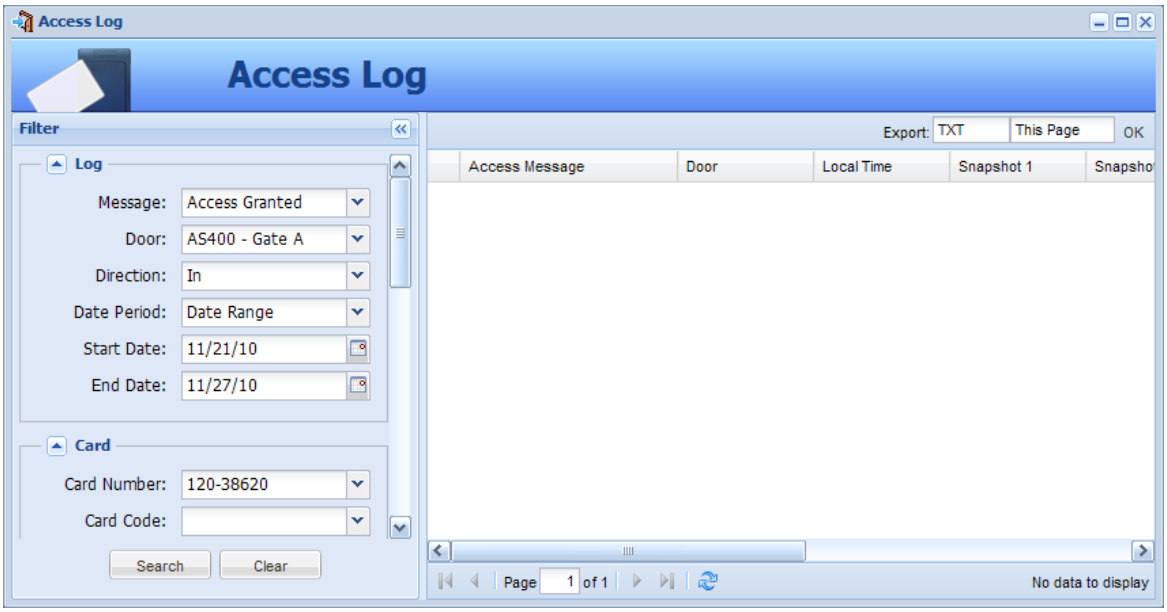


Figure 9-5

3. Click the **Search** button to start the log search.

9.2.2 Log Window Icons

The icons in the log window can display the detailed information of that category. Click the icon to view the details.

: Indicates the availability of the recorded video.

: Indicates the availability of the video image.

In Controller List, Card List, Cardholder List, Access Log and Daily Access, you can right-click each search result to access more information such as card information or cardholder information.

Note: You can play back video only when Remote ViewLog Service included in Control Center Server is enabled on the DVR. And the Remote ViewLog function is enabled on Video Server or Compact DVR.

9.2.3 Exporting Logs

You can download the logs of the connected GV-ASManager to the current computer in three formats: **.txt**, **.htm** and **.xls**.

1. Use the Export drop-down list on the top-right corner and select the file format **TXT**, **HTML** or **Excel**.
2. Use the next drop-down list to select **This Page** to save the current log page or **All** to save all logs.
3. Click **OK** to download the logs.

9.2.4 Defining Columns

You can define the displayed columns of the search results for each type of log. The field must be first enabled on GV-ASManager before the content of the field can become searchable.

1. On the menu bar of the GV-ASManager, click **Tools** and select **ASWeb Field**. This dialog box appears.

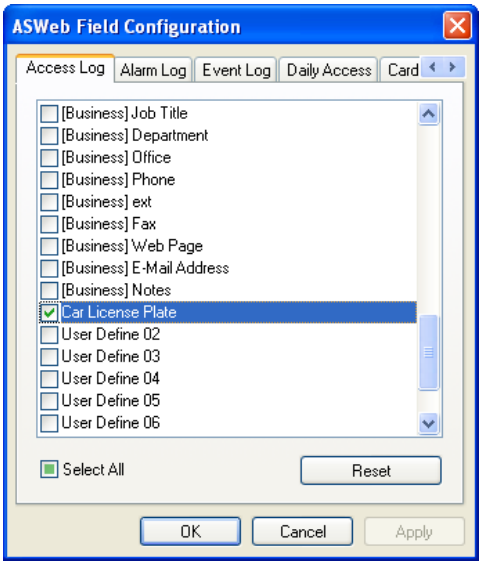


Figure 9-6

2. Select the fields you would like to enable and click **OK**.

3. On GV-ASWeb, click on the arrow next to an existing column and select **Columns**.

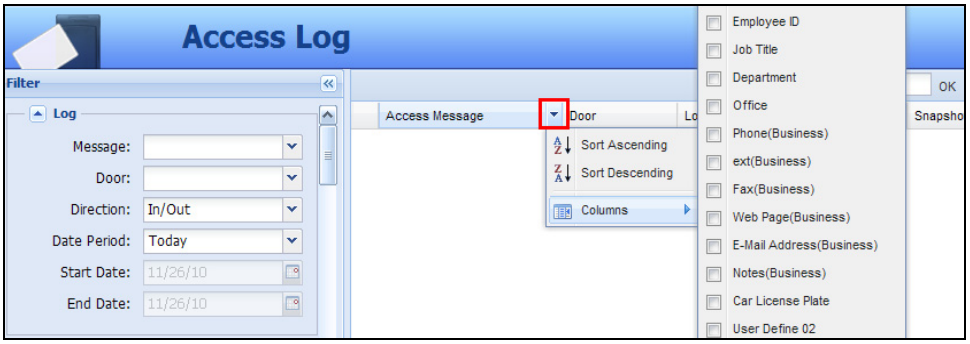


Figure 9-7

4. Select a field to display it in the search results.

   For example, we added a user-defined field “Car License Plate” to the Access Log. The resulting window on the GV-ASWeb may look like this:

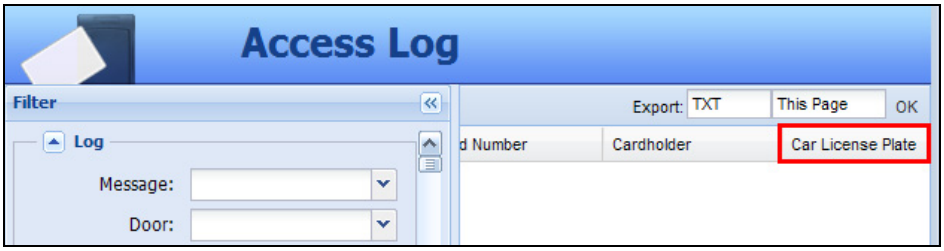
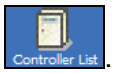


Figure 9-8

9.3 Adding and Deleting Controllers

You can use GV-ASWeb to remotely add or delete controllers to the GV-ASManager.

1. On GV-ASWeb, click the **Controller List** icon 

. This window appears.

Figure 9-9

2. Click the **Add** button to add a new controller. For details on the configurations, refer to *Step 1: Configuring a Controller* in Chapter 4.

3. To set the individual doors, click the **Edit** button and select a door. For details on the configurations, refer to *Step 2: Configuring a Door* in Chapter 4.

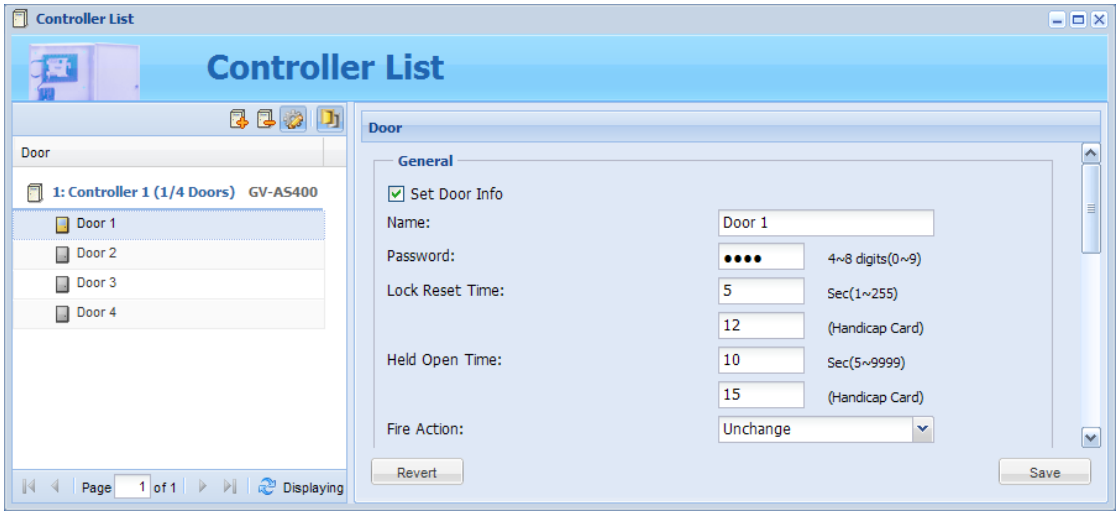


Figure 9-10

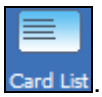
4. To delete a controller, select a controller and click the **Delete** button .

Note: After adding or deleting a controller through GV-ASWeb, the change will be reflected in the Controller List in GV-ASManager.

9.4 Adding and Deleting Cards and Cardholders

In addition to adding and deleting controllers, you can also use GV-ASWeb to remotely add or delete cards and cardholders.

To add or delete cards:

1. On GV-ASWeb, click the **Card List** icon 

.
2. Click the **New** button. This dialog box appears.

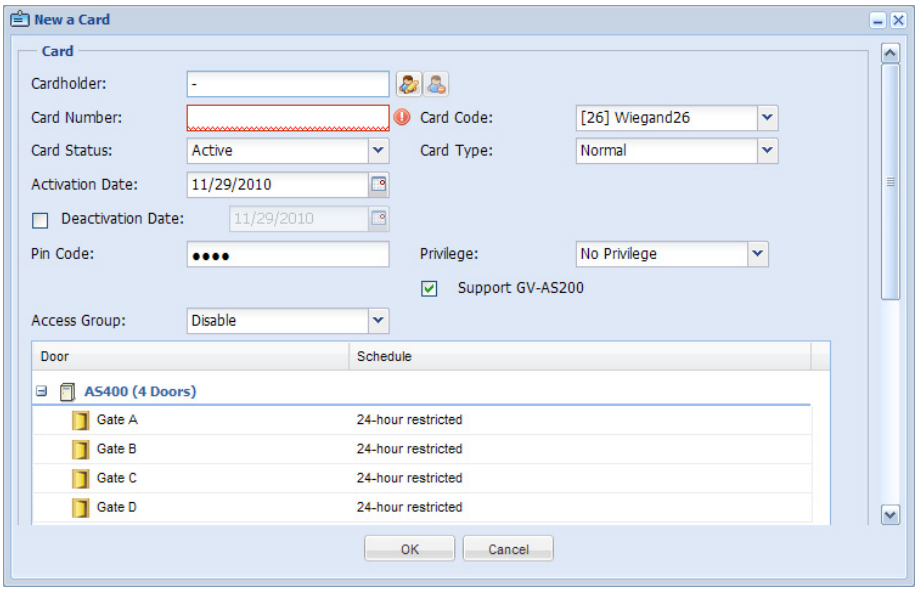


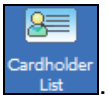
Figure 9-11

3. Fill out the required information. Refer to *4.3 Setting Cards* for more details.
4. Click **OK** to save the settings.
5. To delete cards, simply select the card and click the **Delete** button.

Note:

1. After adding or deleting a card through GV-ASWeb, the change will be reflected in the Card List in GV-ASManager.
2. The Batch function and the card data import/export function are not supported on GV-ASWeb.

To add or delete cardholders:

1. On GV-ASWeb, click the **Cardholder List** icon 

. The Cardholder List window appears.
2. Click the **New** button. This dialog box appears.

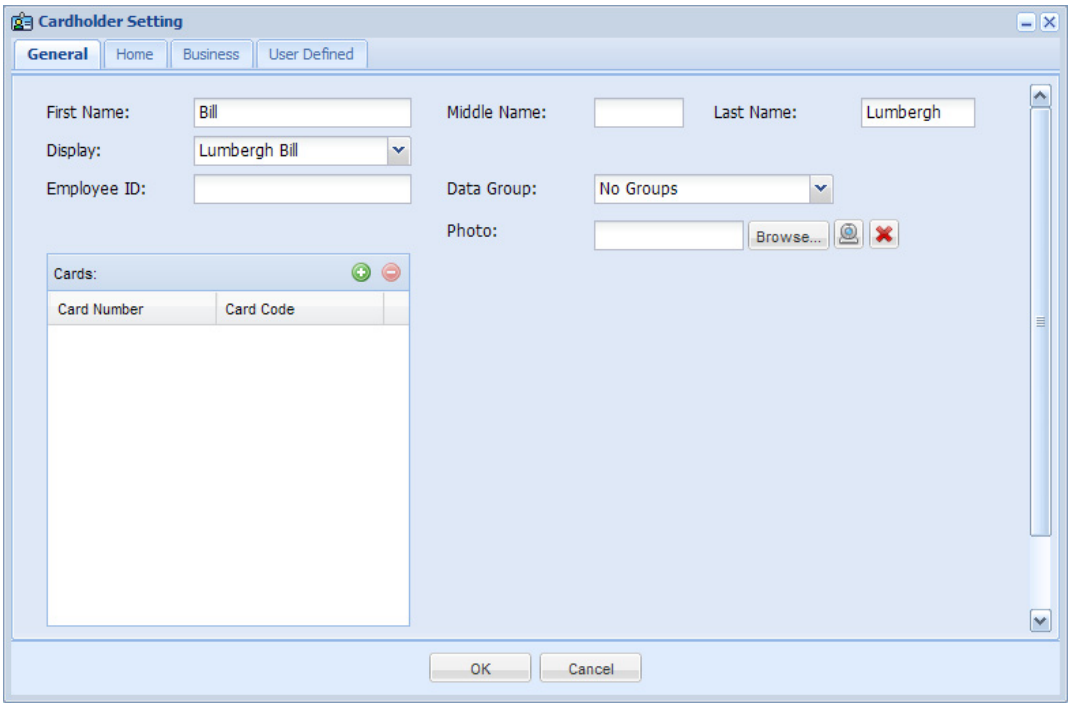


Figure 9-12

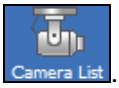
3. Type the cardholder's name. Other cardholder information such as Employee ID, Home information and Business information are optional.
4. You can click the **Add** button to assign a card to the cardholder.
5. If you have a webcam installed, click the **Webcam** icon to take a picture from the Webcam for the cardholder profile.
6. Click **OK** to save the settings.
7. To delete a cardholder, simply select the cardholder and click the **Delete** button.

Note:

1. After adding or deleting a cardholder through GV-ASWeb, the change will be reflected in the Cardholder List in GV-ASManager.
2. The fingerprint enrollment and the cardholder data import / export function are not supported on GV-ASWeb.
3. The webcam function requires Flash Player 10 or later.

9.5 Searching, Adding and Deleting IP Cameras

You can use GV-ASWeb to remotely search and set up IP cameras by connecting to GV-Systems, GV-Video Servers, GV-Compact DVR or to IP cameras directly.

1. On GV-ASWeb, click the **Camera List** icon 

. The Camera List window appears.
2. To search for available IP devices under LAN, click the **Search** button and select **Search DVR and NVR** or **Search IP Device**. This dialog box appears.

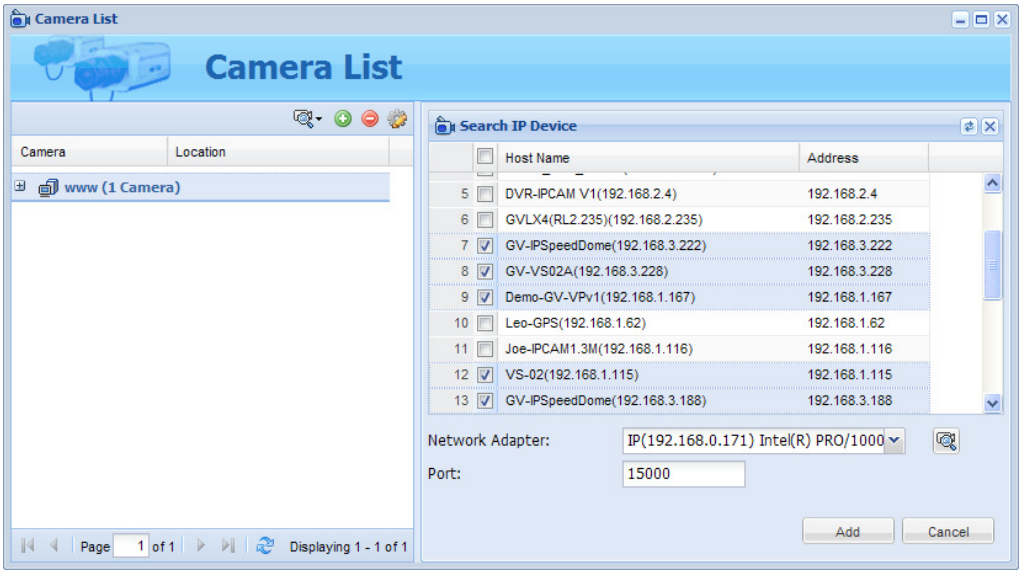


Figure 9-13

A. Select the GV-Systems or IP devices to add from the search results.

B. If necessary, you can select a different **Network Adaptor** and click the **Search** button again or modify the default port number 15000.

C. Click **Add**. The GV-System or IP device is added to the camera list on the left.

D. To login, select the GV-System or IP device, click the **Edit Mode** button , and type the User ID and password.

3. To manually add a device, click the **Add** button . This dialog box appears. *bold

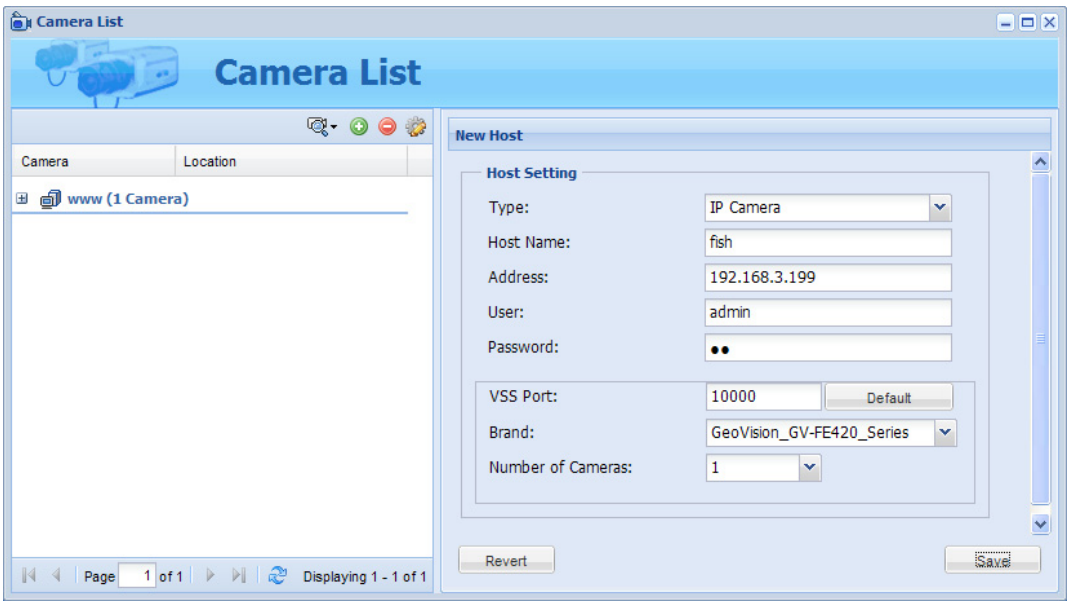


Figure 9-14

A. Select the **Type** of device to add and type a **Host Name** to name the device.

B. Type the IP **Address**, **User** name and **Password** of the device.

C. Modify the default **Data Port** 5611, default **VSS Port** 10000, and default **Log Port** 5552 if necessary.

D. For IP cameras, use the **Brand** drop-down list to select the camera model. You can connect to third-party IP cameras through ONVIF, PSIA and RTSP protocols by selecting **Protocol** in the **Brand** drop-down list.

E. For GV-Systems, GV-Compact DVR and GV-Video Server, select a number from the **Number of Cameras** drop-down list to add channels between channel 1 and the selected channel. For example, if 3 is selected, channels 1-3 will be added.

F. Click **Save**.

4. To edit a device, click the **Edit** button and select a device to begin editing.

5. To delete a device, select the device and click the **Delete** button .

Note: After adding or deleting a camera through GV-ASWeb, the change will be reflected in the Camera List in GV-ASManager.

9.6 Setting Schedule

You can use GV-ASWeb to remotely create daily schedules, set up weekly schedule and specify holidays. For more details on how to set up schedule, refer to Chapter 4.

9.6.1 Setting Daily Schedule

1. On GV-ASWeb, click the **Time Zone Setup** icon

. This dialog box appears.

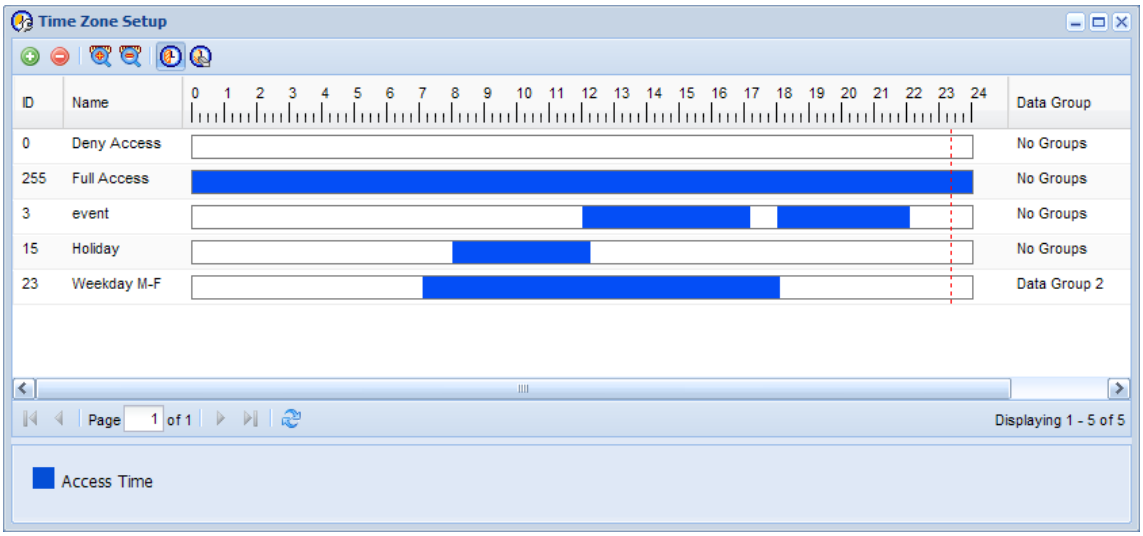

Time Zone Setup
ID
Name
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Data Group
0 Deny Access No Groups
255 Full Access No Groups
3 event No Groups
15 Holiday No Groups
23 Weekday M-F Data Group 2
Page 1 of 1
Displaying 1 - 5 of 5
Access Time

Figure 9-15

2. Click the **Add** button . A blank schedule appears.

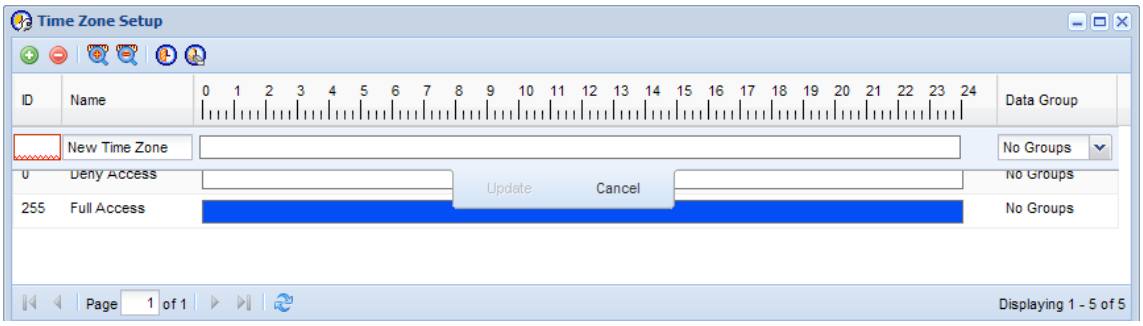
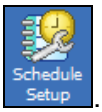

Time Zone Setup
ID
Name
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Data Group
New Time Zone
No Groups
Update
Cancel
255 Full Access
No Groups
Page 1 of 1
Displaying 1 - 5 of 5

Figure 9-16

3. Type an ID and a name for the daily schedule.
4. Set the time by dragging the mouse on the timeline. To erase selected time, click the **Delete Access Time** button and drag the mouse across the selected time.

5. You can use the **Data group** drop-down list to assign the time zone to a data group. You can then allow or forbid a user to read/write the functions listed under the data group. Refer to *Adding a New User* in Chapter 7 for more details.
6. Click **Update** to save.

9.6.2 Setting Weekly Schedule

1. On GV-ASWeb, click the **Schedule Setup** icon 

. This dialog box appears.

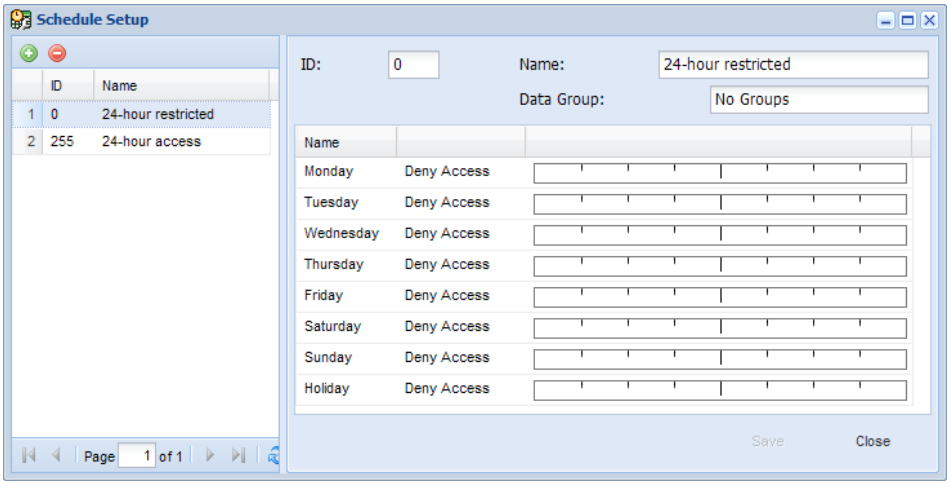
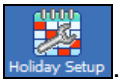


Figure 9-17

2. Click the **Add** button . A blank schedule appears.
3. Type an ID and a name for the weekly schedule.
4. You can use the **Data Group** drop-down list to assign the weekly schedule to a data group. You can then allow or forbid a user to read/write the functions listed under the data group. Refer to *Adding a New User* in Chapter 7 for more details.
5. Click the timeline and assign the daily schedule created to the day of the week. The schedule selected for Holiday will be applied to the dates selected in the Holiday Setup page. Refer to the section below.
6. Click **Save**.

9.6.3 Specifying Holiday

On the main page of GV-ASWeb, click the **Holiday Setup** icon 

. To specify holidays, click **Add Holiday** and click the dates of the Holiday. To remove holidays, click **Remove Holiday** and click the dates.

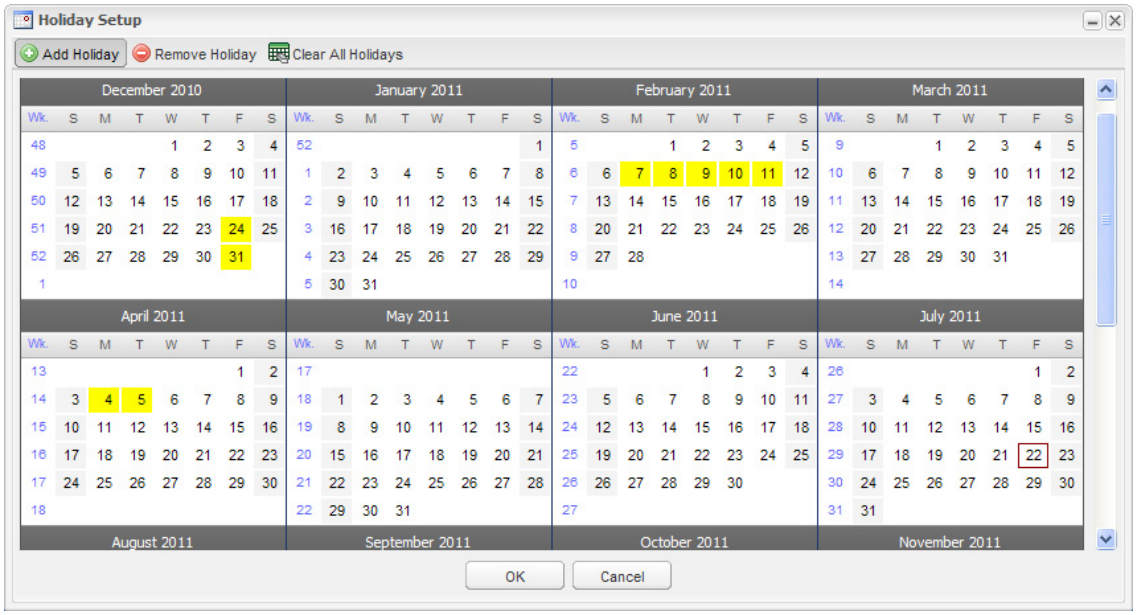
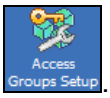


Figure 9-18

9.7 Setting Access Groups

Using GV-ASWeb, you can remotely set up access groups to restrict who can access which door at what time. On the main page of GV-ASWeb, click the **Access Groups** icon 

. For details on how to set up access groups, refer to *Setting Access Groups* in chapter 4.

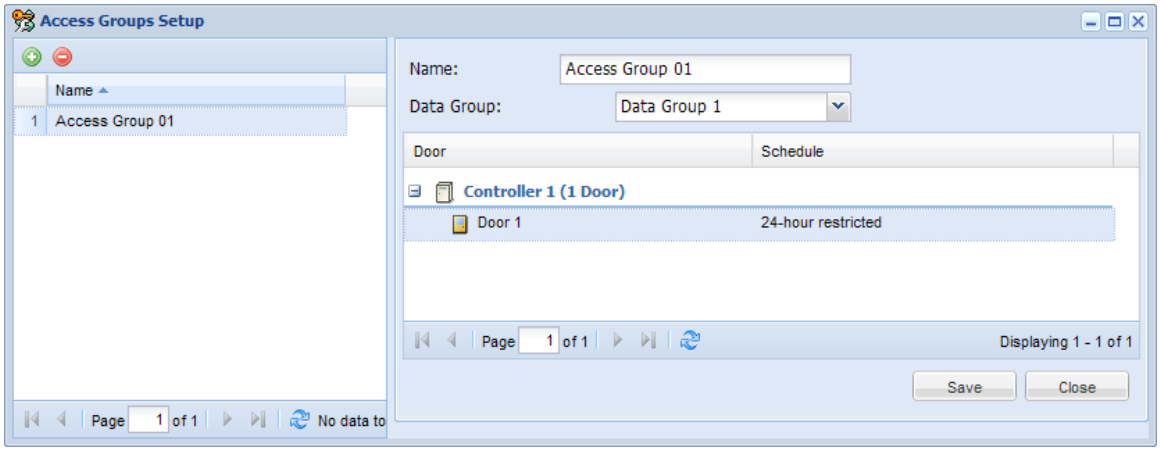
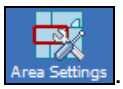


Figure 9-19

9.8 Configuring Areas for Anti-Passback

You can remotely define Entry and Exit areas for each door / gate using GV-ASWeb.

1. On GV-ASWeb, click the **Area Settings** icon 

. This dialog box appears.

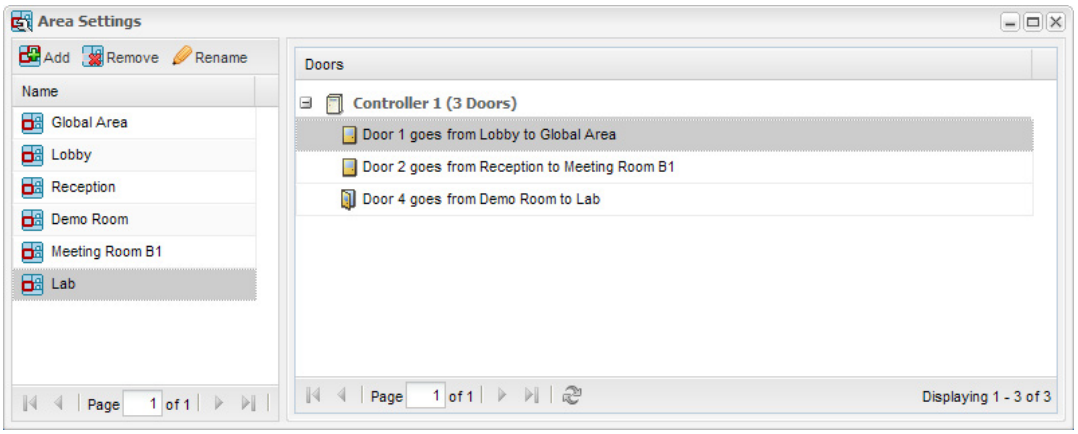


Figure 9-20

2. Click the **Add** button to add an area and double-click the name to rename the area.
3. Double-click a door and use the drop-down lists to assign the entry and exit area.

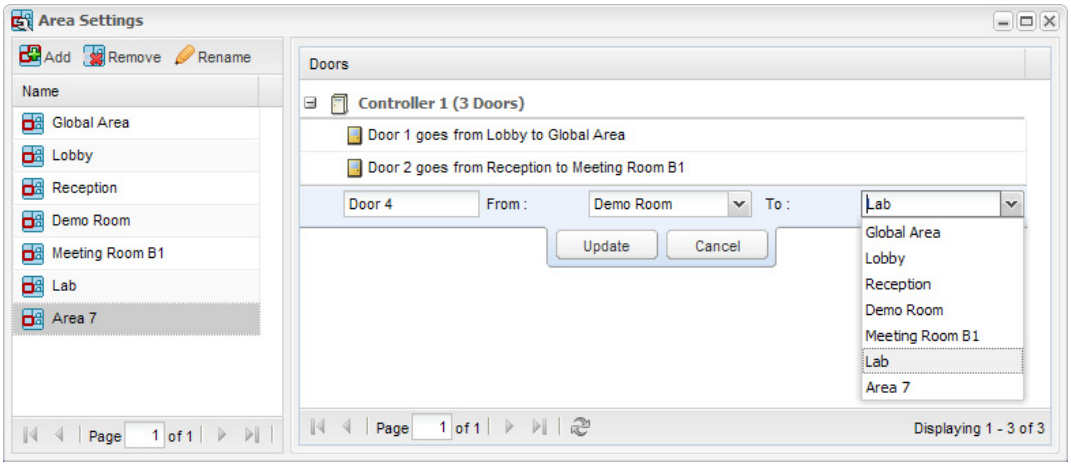


Figure 9-21

For more details on how to set up Anti-Passback, refer to Chapter 6.

Note: After defining areas for Anti-Passback through GV-ASWeb, the change will be reflected in the Area Settings page in GV-ASManager.

9.9 Creating Accounts to Manage GV-ASWeb

The administrator can create accounts with different privileges to manage GV-ASWeb.

1. On the menu bar, click **Tools** and select **Operators**. A dialog box appears.

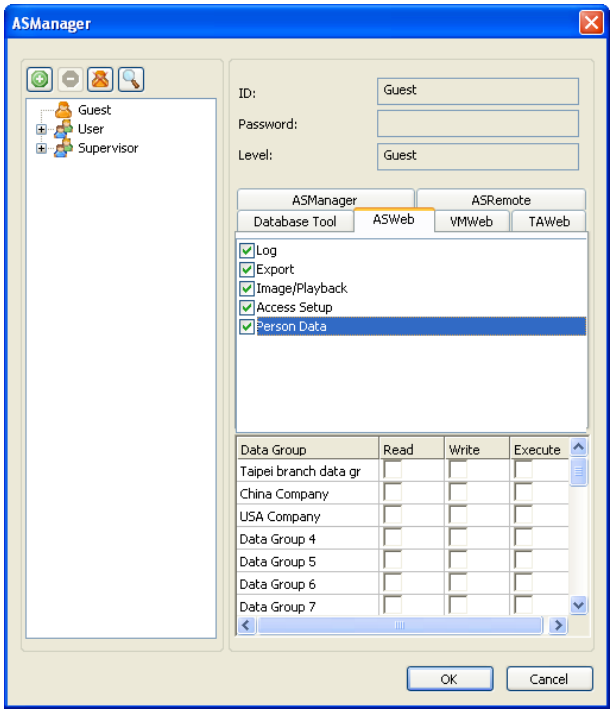


Figure 9-22

2. To create an account, click the **New** button in the top left corner.
3. Type the account's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
4. In the **Level** drop-down list, select **Supervisor** to have access to all GV-ASWeb functions. To grant limited access, select **User**. Click **OK**.
5. Click the **ASWeb** tab in the middle.
6. Select the privileges you want to grant. The following options are available.
   - **Log:** View Alarm Log, Access Log, Daily Access, Event Log and I/O Log.
   - **Export:** Export Alarm Log, Access Log, Daily Access, Event Log and I/O Log.
   - **Image/Playback:** Play back recorded videos and snapshots from GV-ASWeb logs.
   - **Access Setup:** Set up controller list, camera list, area settings, time zone, schedule, holidays and user-defined access group.
   - **Person Data:** Add or edit cards and cardholders.
7. Click **OK**.

Chapter 10 GV-TAWeb for Workforce Schedule and Payoff

GV-TAWeb is a time and attendance management system that helps you assign work shcedule, keep track of employee attendance and calculate salary. You must first enable GV-TAWeb function on GV-ASManager and then log in GV-TAWeb to access the following functions:

- **TA Report:** Looks up workforce schedule, attendance records, and employee payroll.
- **TA Shift:** Sets up different types of daily work schedules.
- **TA Template:** Arranges schedules of up to 45 days with daily schedules from TA Shift.
- **TA Holiday:** Designates which dates are holidays.
- **TA Schedule:** Assigns work schedule to individual or a group of employees.
- **TA User:** Specifies employee salary.

To use the GV-TAWeb, the browser in the client PC must be **Internet Explorer 7 or later**.

10.1 Connecting to GV-ASManager

To enable GV-TAWeb, the **Time Clock** option must be enabled on GV-ASManager and the **Web Server** must be enabled to allow remote access.

1. On the menu bar, click **Setup**, select **Devices** and in the dialog box, double-click the GV-AS Controller you want to use to keep track of attendance. Select the Gate tab and select **Time Clock**.

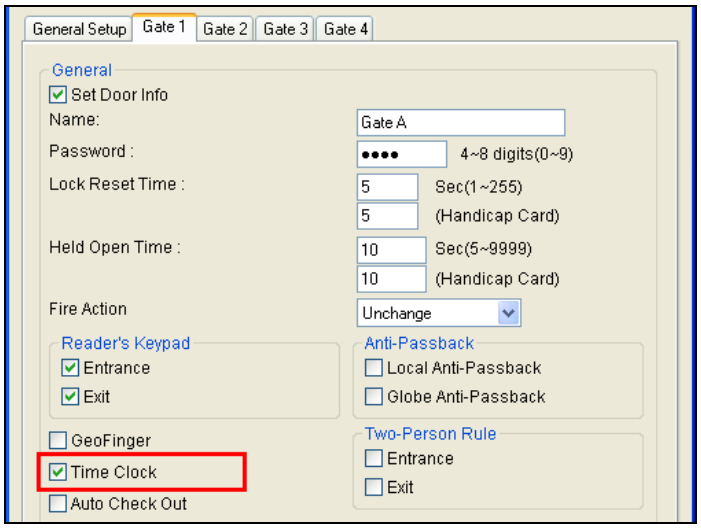


Figure 10-1

2. On the menu bar, click **Tools**, select **Servers** and enable **Web Server**. This dialog box appears.

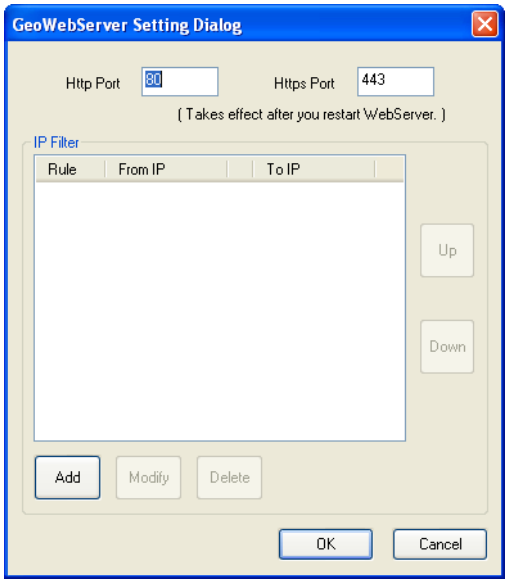


Figure 10-2

If you want to grant or deny the access from certain IP addresses, click **Add**, and type the IP addresses. Otherwise click **OK** to start the connection. When the server is started, the icon appears at the bottom of the main screen.

To start the GV-TAWeb:

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected. This web page appears.

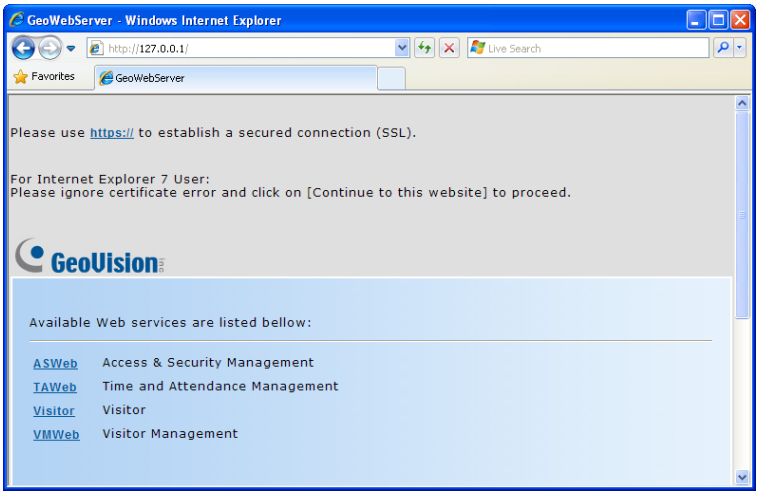

GeoWebServer - Windows Internet Explorer
http://127.0.0.1/
Live Search
Favorites
GeoWebServer
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb Access & Security Management
TAWeb Time and Attendance Management
Visitor Visitor
VMWeb Visitor Management

Figure 10-3

2. Click **https://** for SSL encrypted connection, or **TAWeb** for regular connection.
3. Enter a valid username and password for login. The GV-TAWeb page appears.

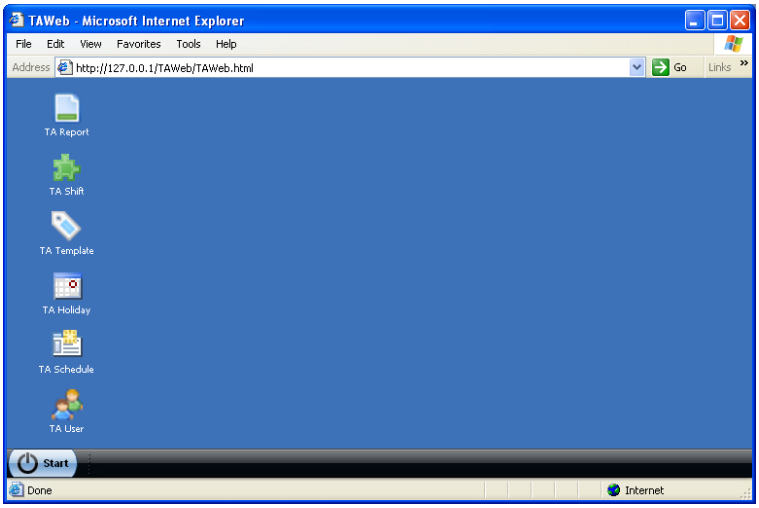


Figure 10-4

10.2 Setting Up Workforce Schedule

To set up workforce schedule, first set up different types of daily work schedule using **TA Shift**, and then you can arrange the different types of daily work schedules into a cycle using **TA Template**. Next, specify the dates for holidays in **TA Holiday**. Lastly, **TA Schedule** allows you to assign work schedule to an employee or a group of employees using daily schedule in TA Shift or using long-term schedule from TA Template.

10.2.1 TA Shift: Setting Up a Daily Schedule

1. Click the **TA Shift** icon. This dialog box appears.

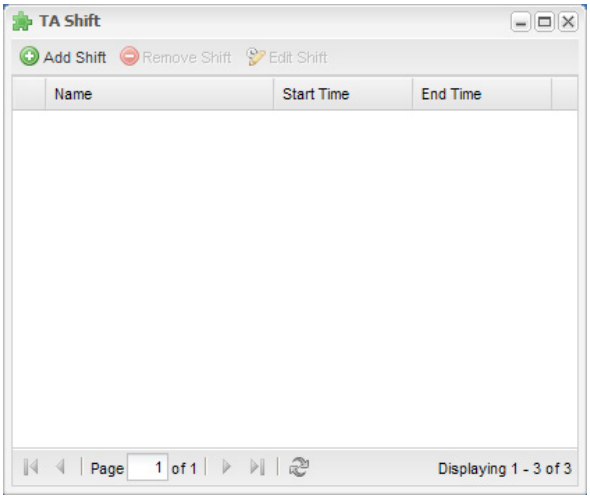


Figure 10-5

2. Click **Add Shift** to add a new daily shift schedule. This dialog box appears.

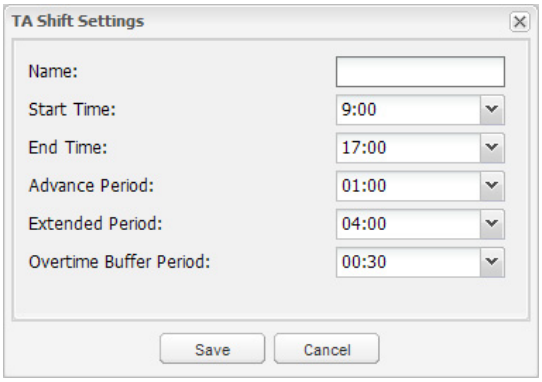


Figure 10-6

3. Type a **Name** for the daily shift to help you identify it.
4. Use the **Start Time** and **End Time** drop-down list to specify when the work shift normally starts and ends.

5. Specify an **Advance Period** to set the amount of time prior to the regular start time an employee can work. Employees arriving before the Advance Period will be recorded as working during Not Scheduled time in TA Record.

6. Specify an **Extended Period** to set the amount of time after the regular end time an employee can work and be counted toward overtime pay. Specify the **Overtime Buffer Period** and an employee has to work passed the overtime buffer period to be counted toward overtime pay.

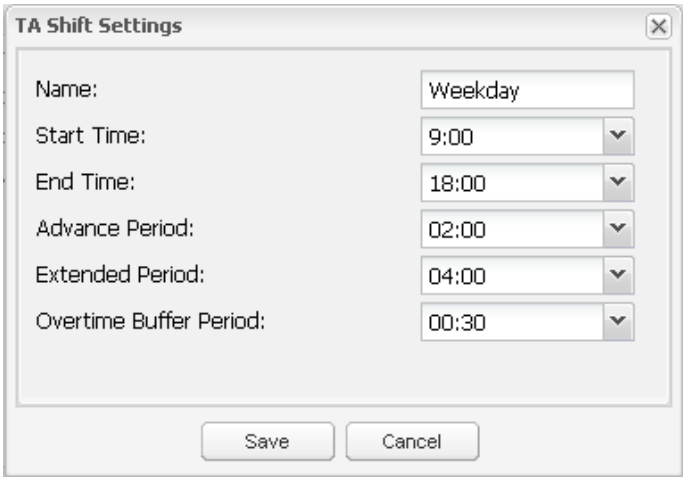


Figure 10-7

Using the above figure as an example, an employee working 4 hours passed the 18:00 pm regular end time will receive overtime pay for 4 hours, while an employee working 20 minutes passed 18:00 will not receive overtime pay.

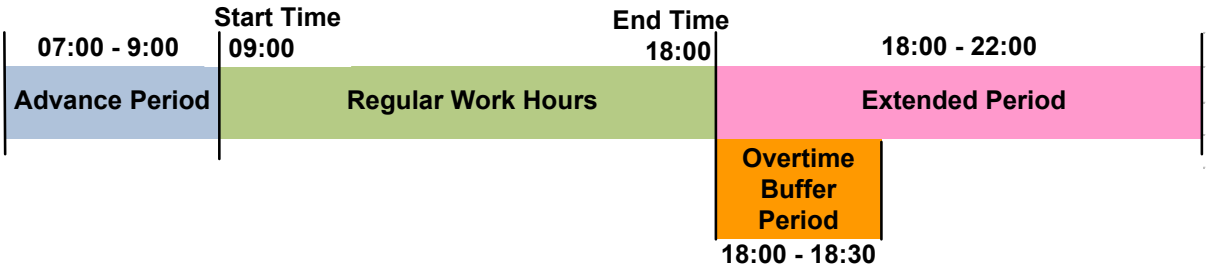


Figure 10-8

7. Click **OK** to save the shift settings.

10.2.2 TA Template: Setting Up a Schedule Template

TA Template allows you to set a 1-45 day recurring schedule template composed of the daily shift schedule created in TA Shift.

1. Click the **TA Template** icon. This dialog box appears.

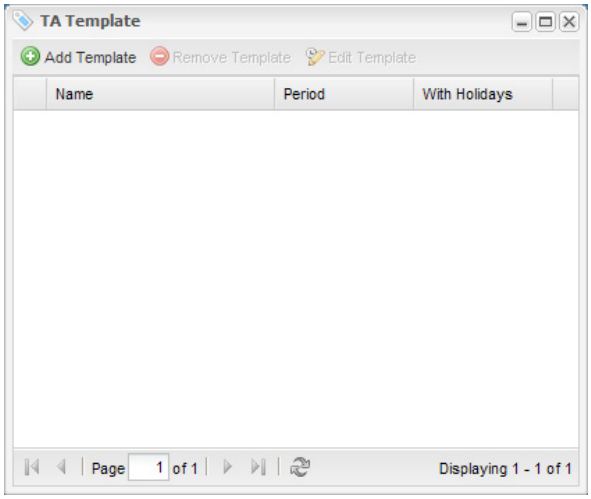


Figure 10-9

2. Click **Add Template**. This dialog box appears.

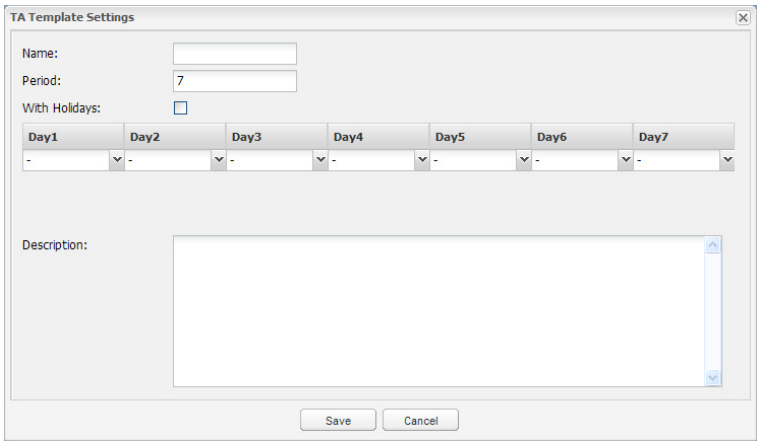


Figure 10-10

3. Type a **Name** to identify the template.
4. In the **Period** field, type a number between 1 and 45 to indicate the number of days in the schedule.
5. Select **With Holidays** to apply the holidays set up in TA Holiday.

6. In the drop-down list below each day, select a daily shift schedule created in TA Shift.

   A TA Template may look like this. In this example, the template is a 2-week work schedule, because the Period is set to 14 days. The drop-down list under each day indicates the daily work schedule selected for that day. A blank drop-down list means that no work schedule is assigned for that day.

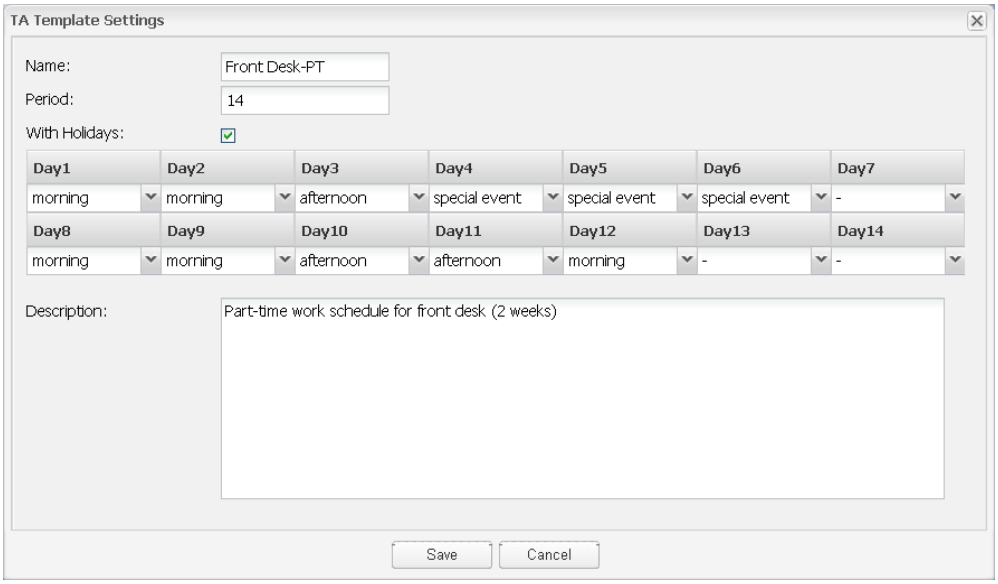


Figure 10-11

7. Click **Save**.

10.2.3 TA Holidays: Setting Certain Dates as Holidays

1. Click the **TA Holiday** icon. This dialog box appears.

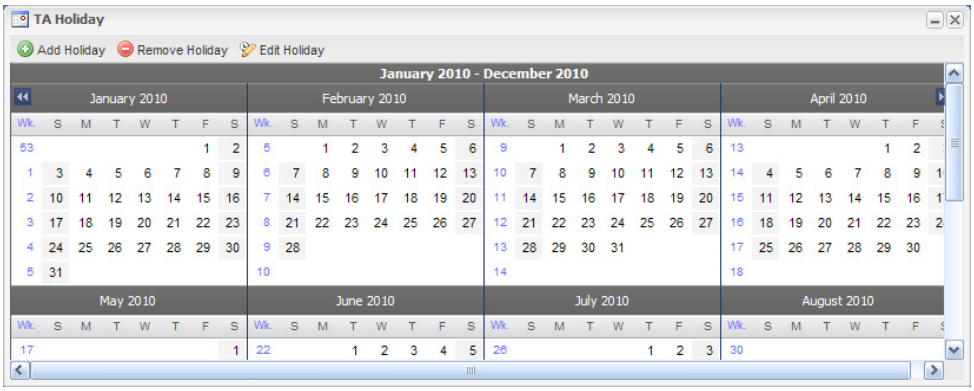


Figure 10-12

2. Select a date and click **Add Holiday**.
3. Type a name for the holiday.
4. Click **OK** and that day will be designated as a holiday if **With Holidays** is selected in TA Template

10.2.4 TA Schedule: Assigning Schedules to Employees

After creating daily shift schedules in TA Shift or arranging a schedule template in TA Template, you can now assign the schedules you set up to an employee or an entire department and select a start date.

Note: The employees listed in TA Schedule are the cardholders in **Cardholder List** on GV-ASManager. To assign employees to a department, open the employees' cardholder information in Cardholder List and select the **Business** tab. In the **Department** field, type the department of the employee and all employees with the same department name will be grouped into one department in GV-TAWeb.

---

1. Click the **TA Schedule** icon. This dialog box appears.

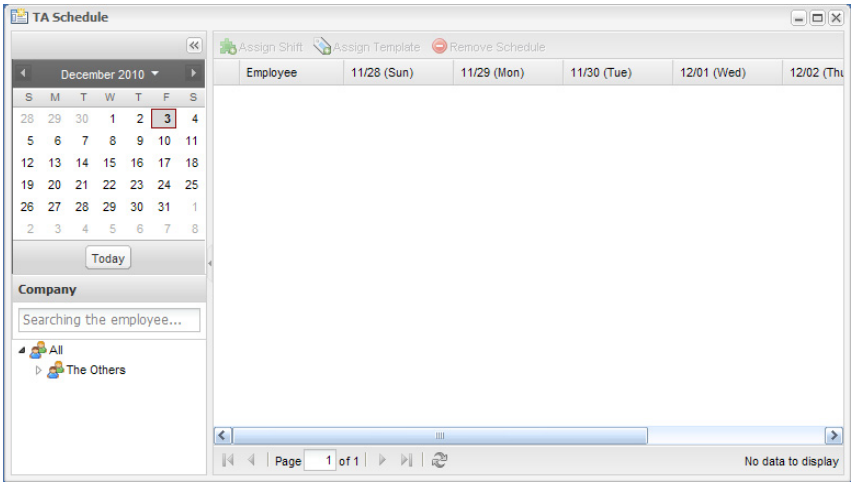


Figure 10-13

To assign daily shift schedules day by day:

2. To assign daily schedules day-by-day, select an employee or a group of employees in the Company section and click **Assign Shift**. This dialog box appears.

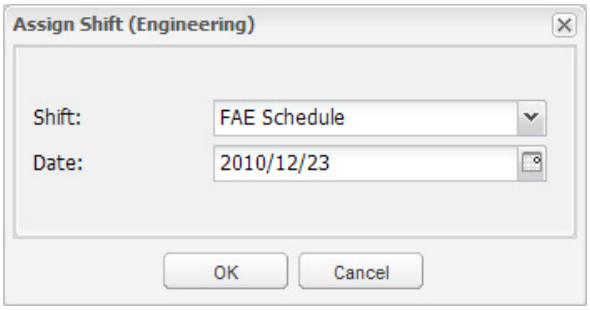


Figure 10-14

3. Select a daily schedule and assign it to a date. Repeat the steps for all the dates you want to schedule a shift.
4. Click **OK**. A TA schedule window may look like this. In this example, different daily schedules created in TA Shift are assigned from Monday to Saturday to two employees.

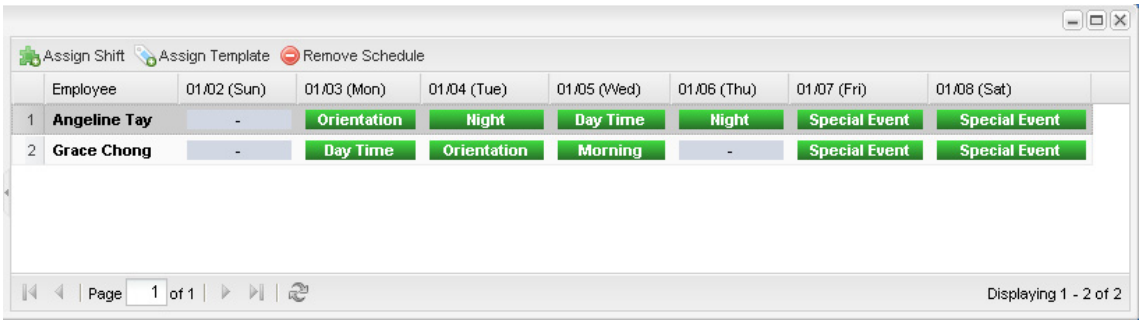


Figure 10-15

To assign a schedule template:

5. To assign a schedule template from TA Template, select an employee or a group of employees and click **Assign Template**. This dialog box appears.

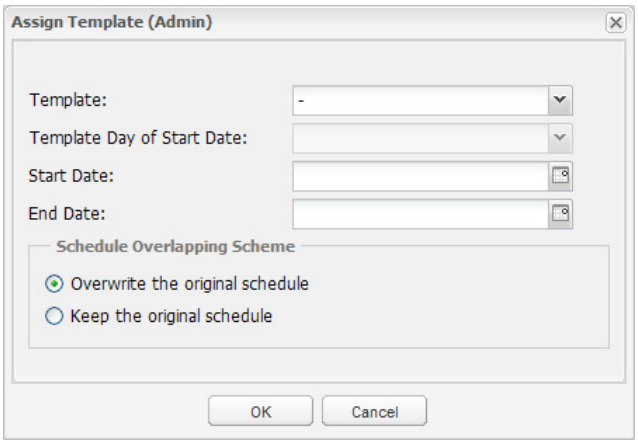


Figure 10-16

6. Using the **Template** drop-down list, select a schedule template created in TA Template.

7. Select a day from the **Template Day of Start Date** drop-down list and the template will start on that day.

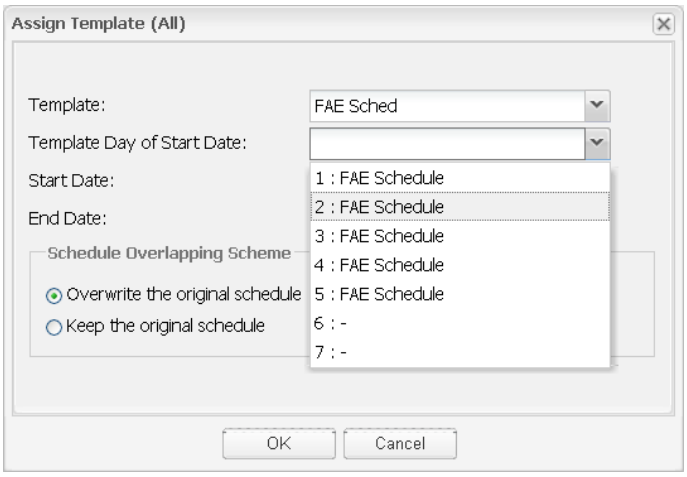


Figure 10-17

8. Select a **Start Date** to begin applying the template and the schedule will begin with the day specified in Template Day of Start Date. Select an **End Date** to discontinue the schedule.

9. In the Schedule Overlapping Scheme section, select **Overwrite the original schedule** if you want to overwrite the original schedule in the case of an overlap.

10. Select **Keep the original schedule** and the template will not be assigned if there is an existing schedule during the time period you specified.

11. Click **OK**. A TA schedule window may look like this. In this example, an FAE weekly schedule created in TA Template are assigned to two employees.

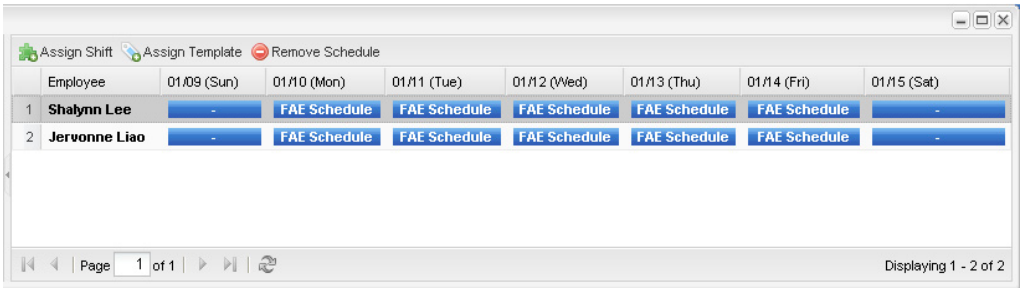

Assign Shift
Assign Template
Remove Schedule
Employee
01/09 (Sun)
01/10 (Mon)
01/11 (Tue)
01/12 (Wed)
01/13 (Thu)
01/14 (Fri)
01/15 (Sat)
1 Shalynn Lee - FAE Schedule FAE Schedule FAE Schedule FAE Schedule FAE Schedule -
2 Jervonne Liao - FAE Schedule FAE Schedule FAE Schedule FAE Schedule FAE Schedule -
Page 1 of 1
Displaying 1 - 2 of 2

Figure 10-18

Hint: To set a weekly schedule with Saturday and Sunday as non-working days, set a 7-day Period and designate two consecutive days as non-working days by not selecting a daily shift.

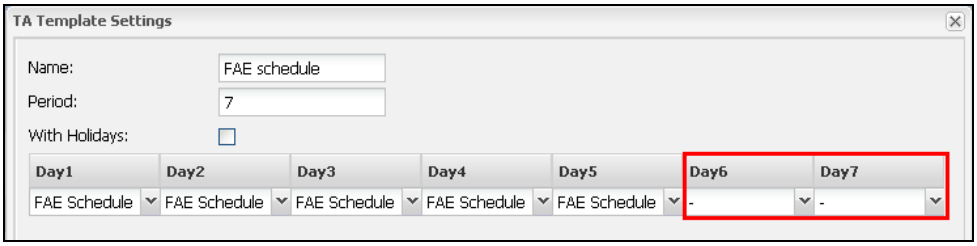
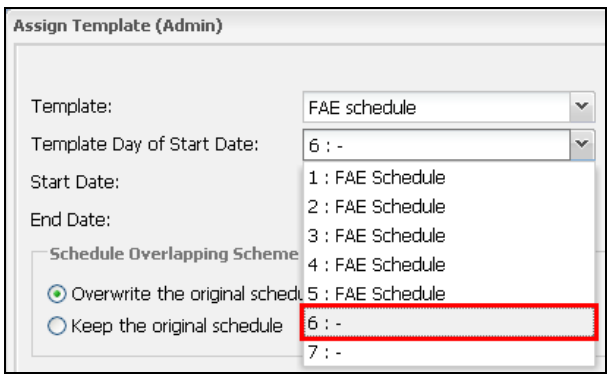
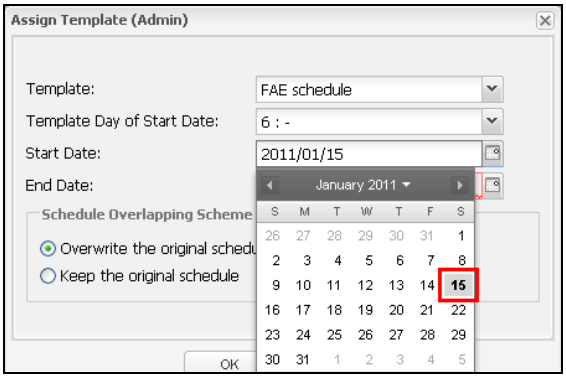


Figure 10-19

Then, in TA Schedule, match the first non-working day with a Saturday.



Select the first non-working day



Select a Saturday for Start Date

Figure 10-20

10.3 TA User: Specifying Hourly Pay

You can specify the hourly pay for regular work hours and overtime work hours using **TA User**.

1. Click the **TA User** icon. This dialog box appears.

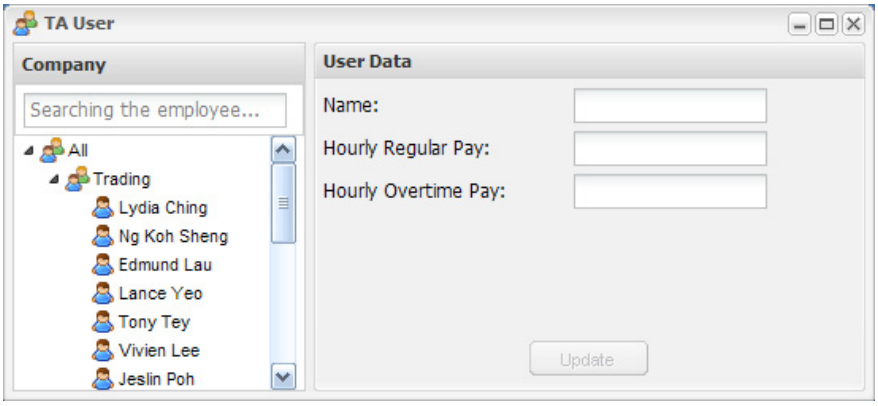


Figure 10-21

2. Select an employee from the list.
3. Type the **Hourly Regular Pay** and the **Hourly Overtime Pay**.
4. Click **Update** to save the settings.

Note: The employees listed in TA User are the cardholders in the Cardholder List. To see how to add, edit or delete cardholders, refer to *4.6 Setting Cardholders*.

10.4 TA Report: Looking Up Records

TA Report allows you to look up workforce schedules, attendance record, payroll and summaries of each department's data.

1. Click the **TA Report** icon. This dialog box appears.

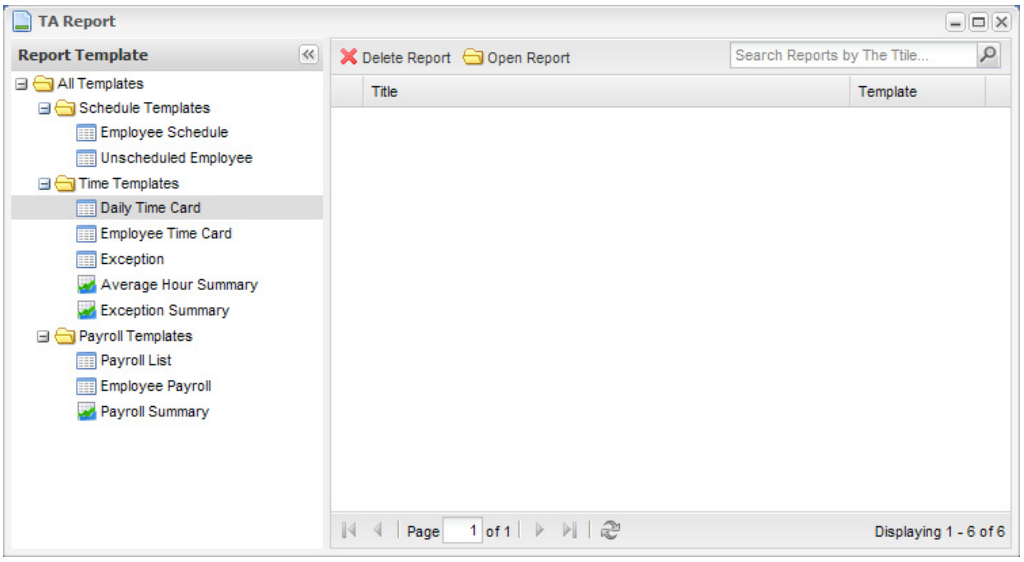


Figure 10-22

2. On the left panel, the following data and graphs are available:

Note: Accessing **Average Hour Summary**, **Exception Summary** or **Payroll Summary** requires Flash Player 10 or later.

[Schedule Templates]

- **Employee Schedule:** Shows the work schedule of an individual employee.
- **Unscheduled Employee:** Shows the days when employees are not scheduled to work.

[Time Templates]

- **Daily Time Card:** Shows the work schedule and the actual punch in/out time of employees in a department.
- **Employee Time Card:** Shows the work schedule and the actual punch in/out time of an individual employee.

- **Exception:** Searches for records within a department of the events selected. The following Exception Events are available for selection:
  - **In Late:** Punching in after the assigned start time.
  - **In Early:** Punching in before the assigned start time.
  - **Out Late:** Punching out after the assigned end time.
  - **Out Early:** Punching out before the assigned end time.
  - **Over Hours:** Working after the Overtime Buffer Period but before the Extended Period.
  - **Unscheduled Absence:** Absence during scheduled work day.
  - **Missed Punch:** Punching in without punching out or punching out without punching in.
  - **Not Scheduled:** Working on days when there is no assigned shift for that day.
- **Average Hour Summary:** Shows each department's average work hours per person during the time period specified and the percentage occupied in comparison to other departments.
- **Exception Summary:** Displays a department's total counts of Exception Events within the time period specified.

[Payroll Templates]

- **Payroll List:** Shows the hourly pay, total work hours and total pay of the employees within a department during the time period specified.
- **Employee Payroll:** Shows the hourly pay, total work hours and total pay of an employee for each day of the time period specified.
- **Payroll Summary:** Shows the average total pay of each department during the time period specified and the percentage occupied within the company.

3. Using the Daily Time Card as an example, double-click **Daily Time Card** on the left menu and this dialog box appears.

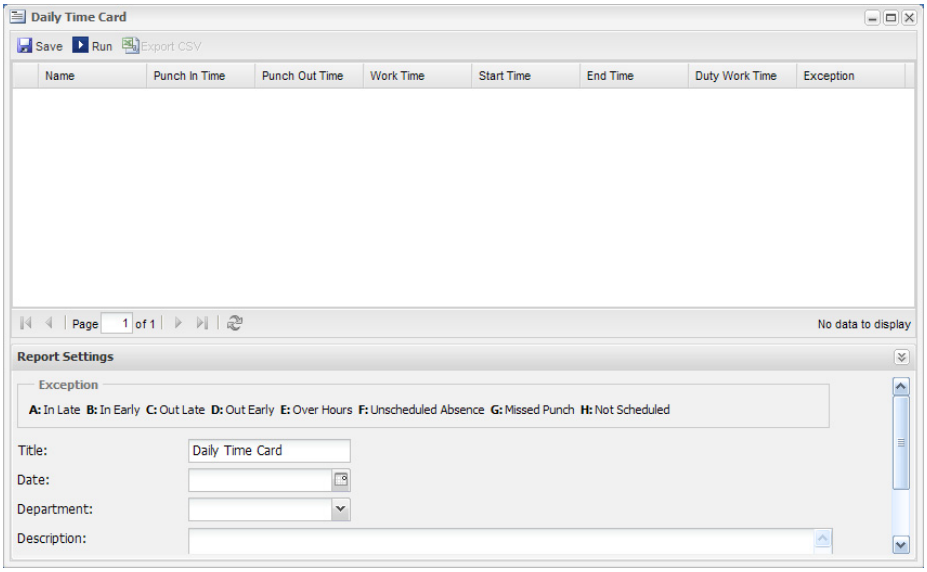


Figure 10-23

4. Select the **Date** and **Department** to look up the employees' scheduled shift and actual attendance record.

5. Click the **Run** button toward the top. A dialog box similar to the one below appears. Using the first person as an example, Lydia punched in at 10:01 and punched out at 16:56, even though her scheduled work time is from 9:00 to 17:00. She is therefore listed as A (In Late) and D (Out Early) in the **Exception** column. The number of hours she worked is listed under the **Work Time** column.

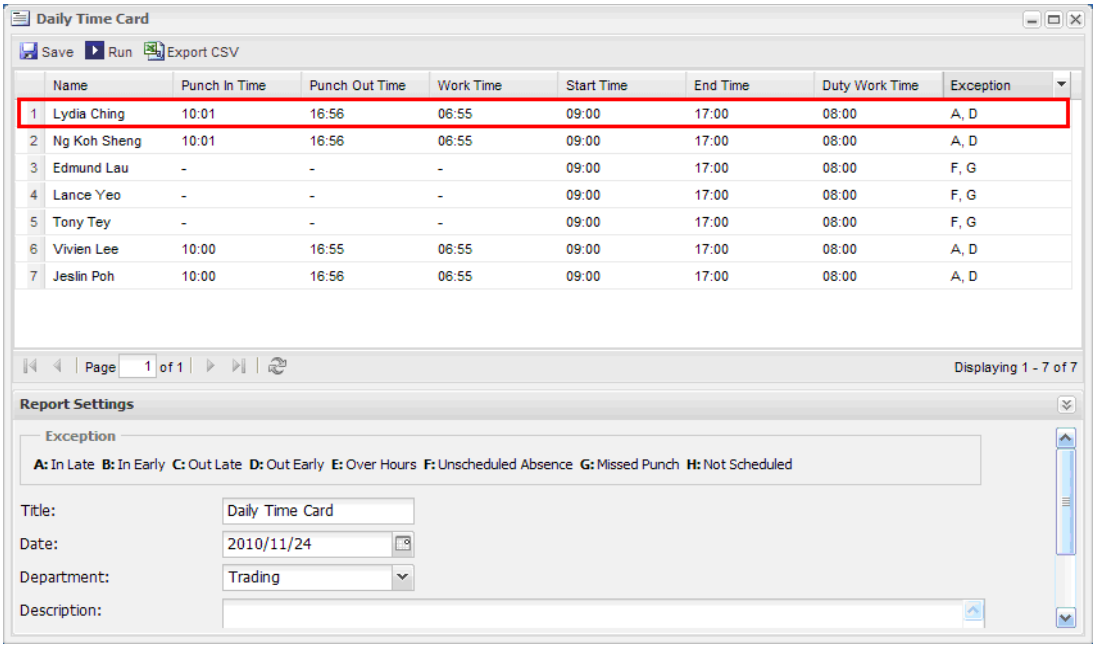

Daily Time Card
Save
Run
Export CSV
Name
Punch In Time
Punch Out Time
Work Time
Start Time
End Time
Duty Work Time
Exception
1 Lydia Ching 10:01 16:56 06:55 09:00 17:00 08:00 A, D
2 Ng Koh Sheng 10:01 16:56 06:55 09:00 17:00 08:00 A, D
3 Edmund Lau - - - 09:00 17:00 08:00 F, G
4 Lance Yeo - - - 09:00 17:00 08:00 F, G
5 Tony Tey - - - 09:00 17:00 08:00 F, G
6 Vivien Lee 10:00 16:55 06:55 09:00 17:00 08:00 A, D
7 Jeslin Poh 10:00 16:56 06:55 09:00 17:00 08:00 A, D
Page 1 of 1
Displaying 1 - 7 of 7
Report Settings
Exception
A: In Late B: In Early C: Out Late D: Out Early E: Over Hours F: Unscheduled Absence G: Missed Punch H: Not Scheduled
Title:
Daily Time Card
Date:
2010/11/24
Department:
Trading
Description:

Figure 10-24

6. Click **Save** and a shortcut of the Daily Time Card for the specified department and date will be created in the TA Report main page.

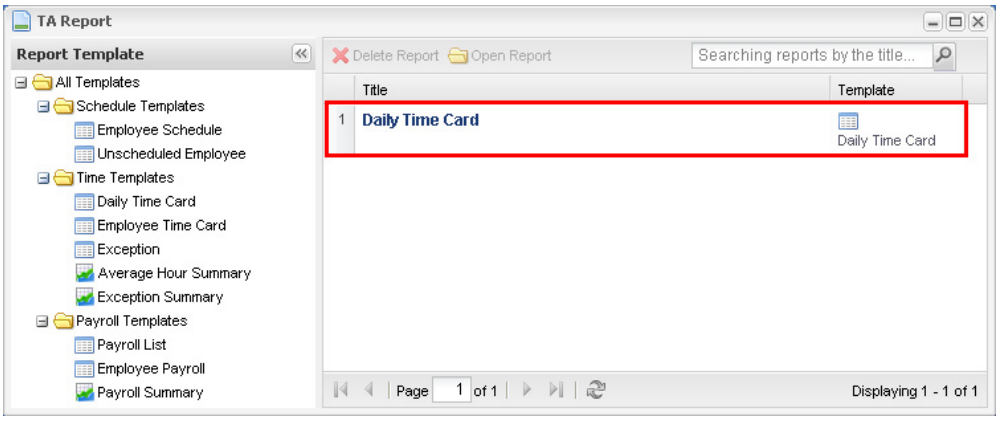


Figure 10-25

7. Click **Export CSV** to export the data in an excel file.

8. To select which data to display, click the arrow next to the column title and click **Column**.

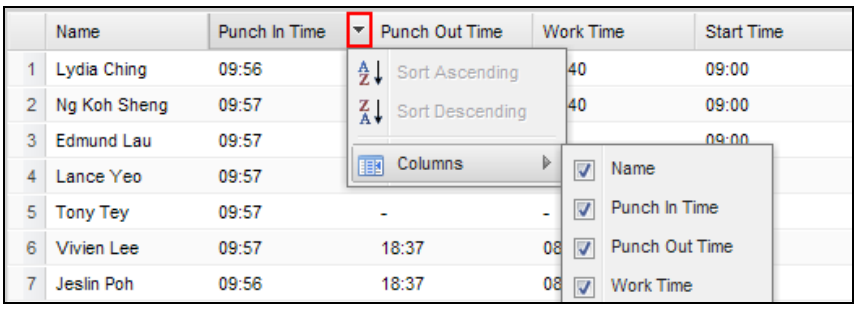


Figure 10-26

Note: The **Export CSV** function is only available after you have saved the report by clicking the **Save** button.

10.5 Creating Accounts to Manage GV-TAWeb

The administrator can create accounts with different privileges to manage GV-TAWeb.

1. On the menu bar, click **Tools** and select **Operators**. A dialog box appears.

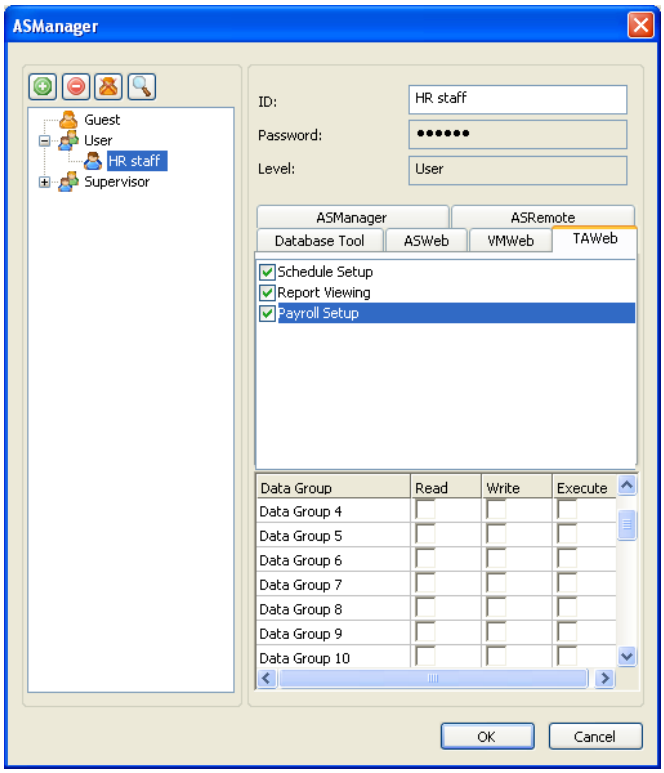


Figure 10-27

2. To create an account, click the **New** button in the bottom left corner.
3. Type the account's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
4. In the **Level** drop-down list, select **Supervisor** to have access to all GV-TAWeb functions. To grant limited access, select **User**. Click **OK**.
5. Click the **TAWeb** tab.
6. Select the privileges you want to grant. The following options are available.
   - **Schedule Setting:** Access TA Shift, TA Template and TA Schedule.
   - **Report viewing:** Access TA Report.
   - **Payroll settings:** Access TA User.
7. Click **OK**.

Chapter 11 GV-VMWeb for Visitor Management

The GV-VMWeb is a visitor management system for internal business use where the administrator can create a visitor database and grant access to visitors on a LAN environment. GV-VMWeb can also be set up to allow visitors to register their own visitor account and create visit requests over the internet using the Visitor service.

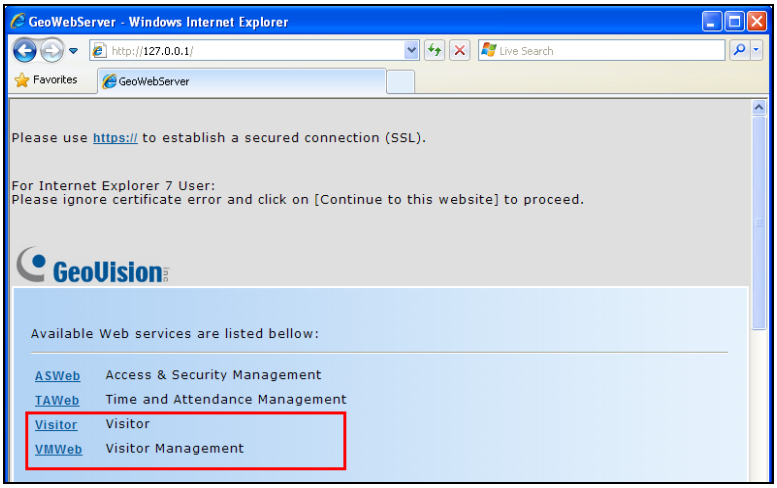

GeoWebServer - Windows Internet Explorer
http://127.0.0.1/
Favorites
GeoWebServer
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb Access & Security Management
TAWeb Time and Attendance Management
Visitor Visitor
VMWeb Visitor Management

Figure 11-1

To use the GV-VMWeb, the browser in the client PC must be **Internet Explorer 7 or later**.

11.1 Connecting to GV-ASManager

Before GV-VMWeb can connect to a GV-ASManager, remote access must be enabled on the GV-ASManager as below:

- On the menu bar, click **Tools**, select **Servers** and enable **Web Server**. This dialog box appears.

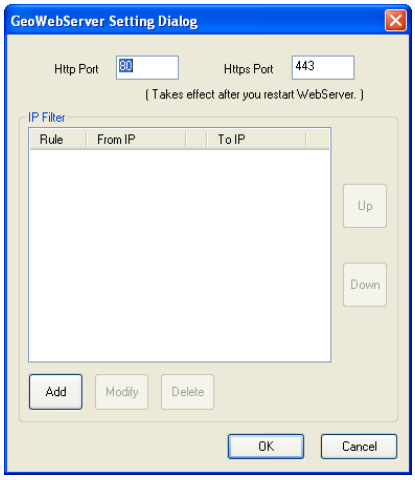


Figure 11-2

If you want to grant or deny the access from certain IP addresses, click **Add** and type the IP addresses. Otherwise click **OK** to start the connection. When the server is started, the icon appears at the bottom of the main screen.

To start the GV-VMWeb:

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected. This web page appears.

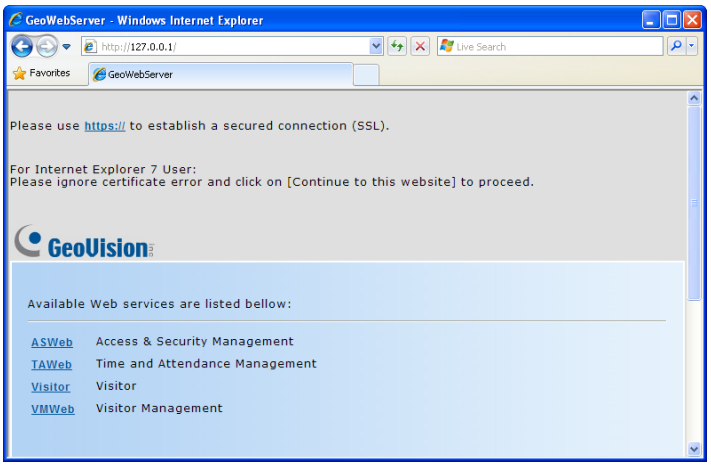

GeoWebServer - Windows Internet Explorer
http://127.0.0.1/
Favorites
GeoWebServer
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb Access & Security Management
TAWeb Time and Attendance Management
Visitor Visitor
VMWeb Visitor Management

Figure 11-3

2. Click **https://** for SSL encrypted connection, or **VMWeb** for regular connection.
3. Enter a valid username and password for login. The GV-VMWeb page appears.

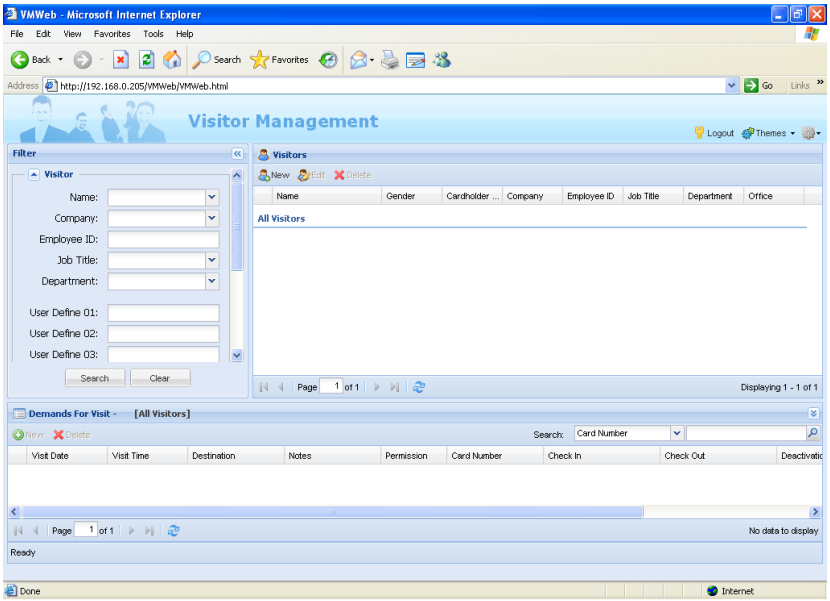
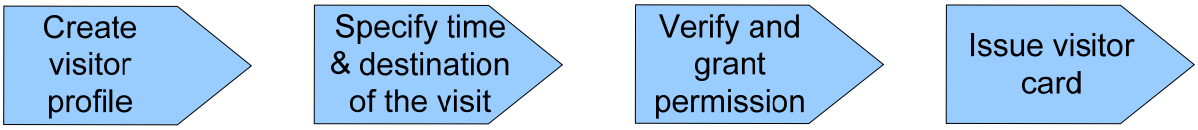


Figure 11-4

11.2 Creating Accounts to Manage GV-VMWeb

The administrator can create multiple accounts with different privileges to manage each step of granting access as shown below.



You can create a security staff account with privileges to create **Visitor Data** and **Visit Records**, while another account with privileges to **Verify** visitors and **Issue Card** can be assigned to a management staff. In this setup, the security staff can create a visitor profile and a visit request for visitors, but the management staff needs to approve the visit and issue a card to the visitor before the visitor can be granted access.

Note: You need to create a visitor card before you can issue a card to a visitor. To see how to add a visitor card, refer to *4.3 Adding Cards*.

To create accounts:

1. On the menu bar, click **Tools** and select **Operators**. This dialog box appears.

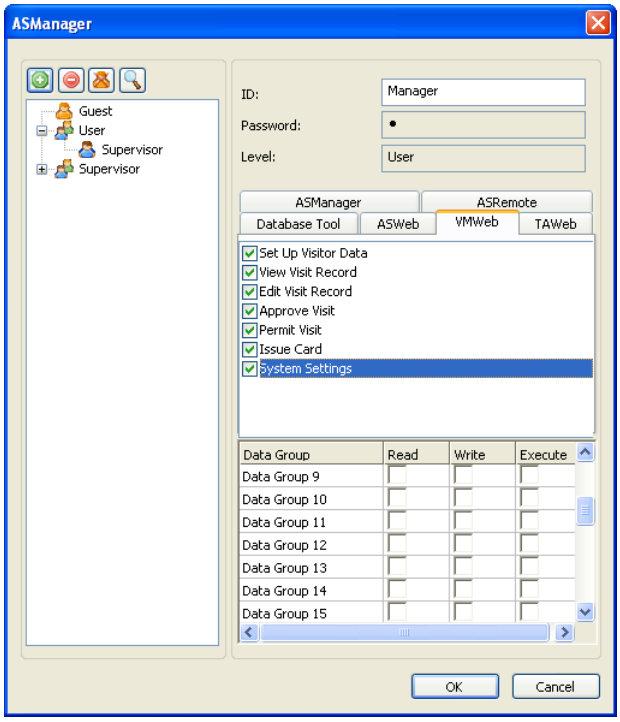


Figure 11-5

2. To create an account, click the **New** button in the bottom left corner. This dialog box appears.

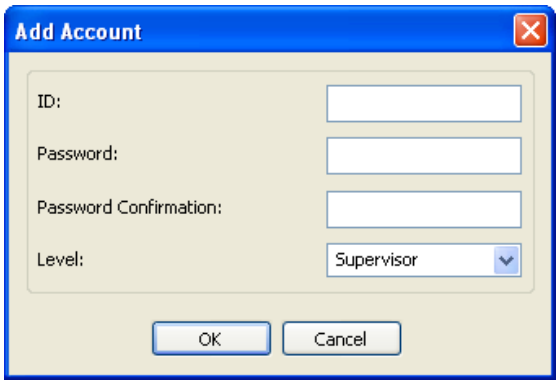


Figure 11-6

3. Type the Supervisor's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
4. In the **Level** drop-down list, select **Supervisor** to have access to all GV-VMWeb functions as shown in Figure 11-6. Click **OK**. To grant limited access, select **User** and click **OK**.
5. Click the **VMWeb** tab.
6. Select the privileges you want to grant. The following options are available.
   - **Set Up Visitor Data:** Create or edit visitor profiles.
   - **View Visit Record:** Look up visit records in the past for each visitor.
   - **Edit Visit Record:** Create or edit visits in GV-VMWeb.
   - **Approve Visit:** Record the name of the account that approved the visit request.
   - **Permit Visit:** Grant permission to allow the visit in GV-VMWeb
   - **Issue Card:** Assign a card to the visitor in GV-VMWeb. The Verify privilege must also be allowed for the account to have access to this option.
   - **System Settings:** Enable the Auto-Verify option under **Setting** drop-down list .
7. Click **OK**.

11.3 Creating Visitor Profile

GV-VMWeb allows you to create visitors profile and grant different access to each visitor.

To create a visitor account:

1. In the Visitor section, click the **New** button. This dialog box appears.

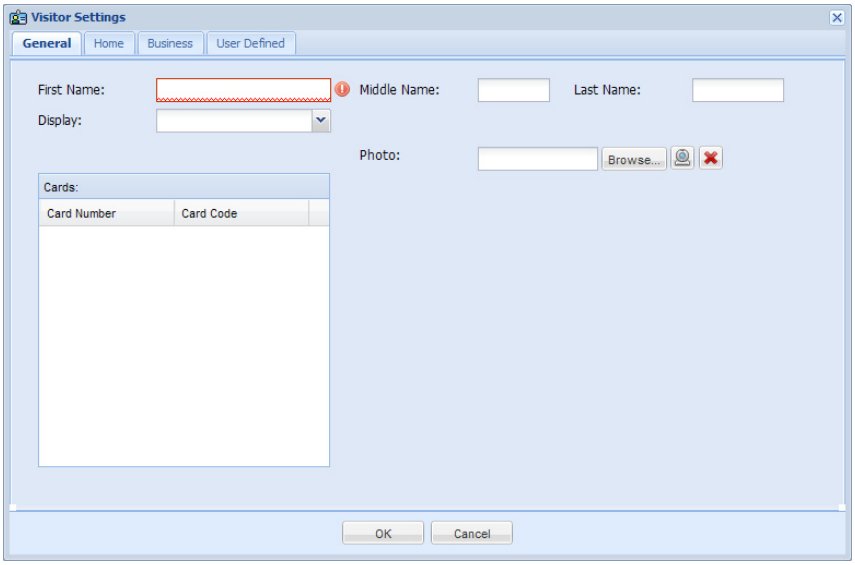


Figure 11-7

2. In the **General** tab, you can type the name of the visitor and click **Browse** to upload a photo of the visitor. If you have a webcam installed, click the **Webcam** icon to take a picture from the webcam for the visitor profile. Any valid card number and card code for the visitor will be displayed under the **Cards** section.
3. In the **Home** and **Business** tab, you can fill out other personal information about the visitor, such as phone number, address, birthday and gender.
4. In the **User Defined** tab, customized field labels will be displayed. To see how to customize the fields, see *4.6.4 Customizing a Data Field*.
5. Click **OK** to save the visitor information.

Note:

1. The visitor profile created will be updated to the Cardholder List in GV-ASManager.
2. The webcam function requires Flash Player 10 or later.

11.4 Granting Visitor Access

After the visitor's account is created, access permission can be granted to visitors using the **Demand for Visits** section. In this section, you can specify the date and time of the visit, assign an access card to the visitor and view visit record.

1. Select the visitor account in the Visitors section and click the **New** button in the Demands for Visit section.

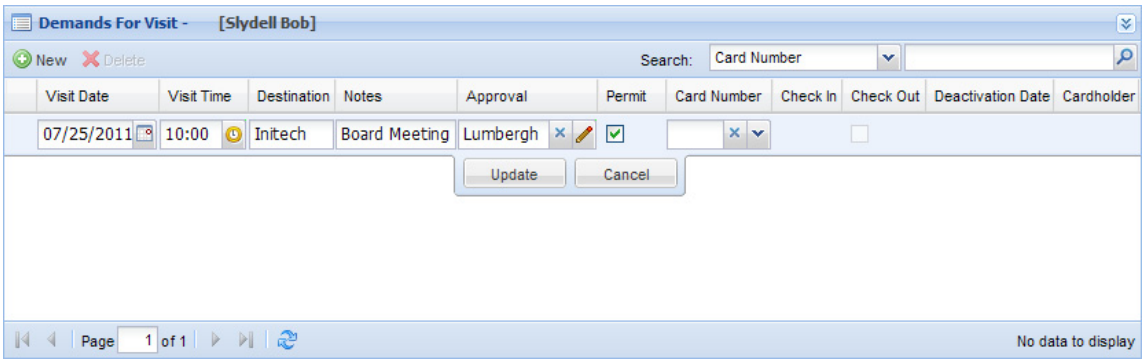


Figure 11-8

2. Select a **Visit Date** and **Visit Time** to note the time when the visitor will be visiting.
3. You can type a **Destination** and **Note** for your own reference.
4. Under **Approval**, click the button to note the name of the account that permitted the access.
5. Select the **Permit** checkbox to grant access permission.
6. Click the **Card Number** drop-down list. This dialog box appears.

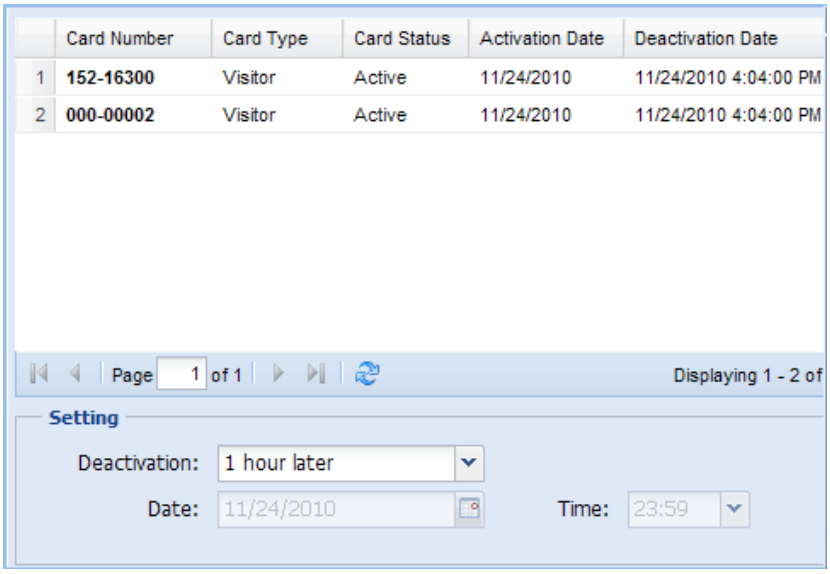


Figure 11-9

Note: You need to first create a visitor card before you can issue a card to a visitor. To see how to add a visitor card, refer to *4.3 Adding Cards*.

7. Select a visitor card to assign to the visitor and use the **Deactivation** drop-down list to specify when the card will be deactivated.
8. Click the **Update** button to continue editing the Demand for Visit entry.
9. The **Check-In** time is the time when the Demand for Visit entry is created. After the visitor has returned the visitor card, you can return to this visit record and select the **Check-Out** checkbox to check out the card. You can also choose to automatically check out the visitor card when the visitor presents the card at an exit door. Refer to *Step 2: Configuring a Door* in Chapter 4 to see how to set up automatic check out.

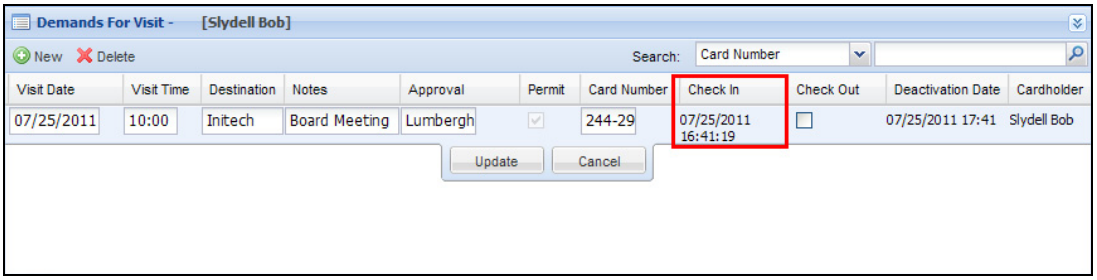


Figure 11-10

10. Click the **Update** button to save the settings and the data will be updated to GV-ASManager.

11.5 Searching GV-VMWeb Database

To search for visitors with certain criteria, type the visitor's information in the **Filter** section on the left and click the **Search** button. The search results will be listed in the **Visitors** section. You can also search visit records from the past by using the **Search** function under Demands For Visit section. Use the drop-down list to search by Card Number, Destination, Notes or Cardholder.

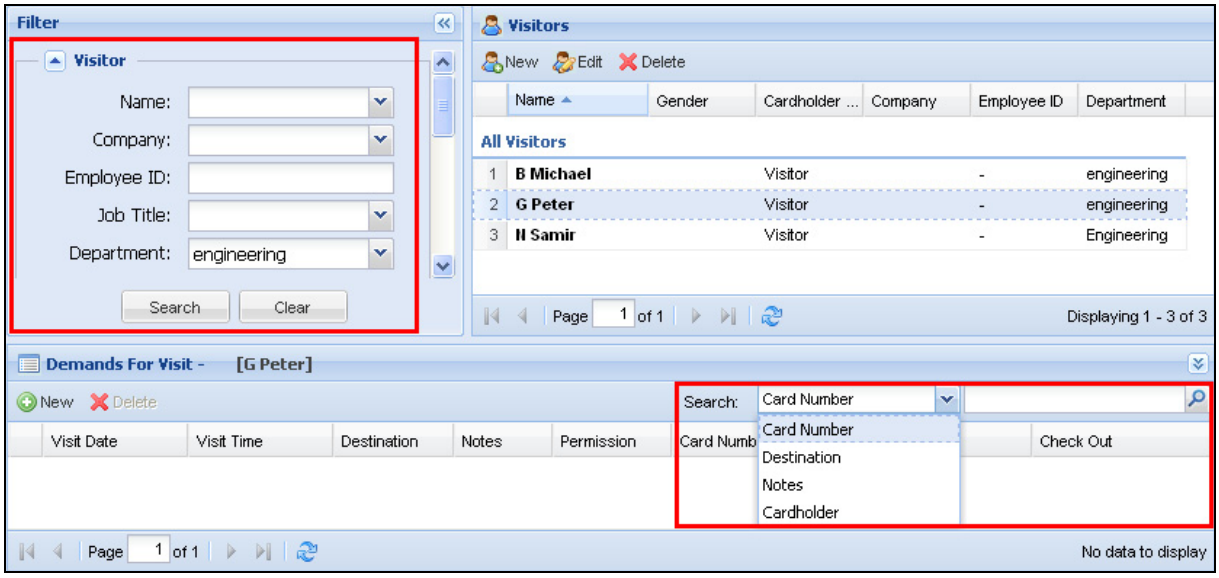
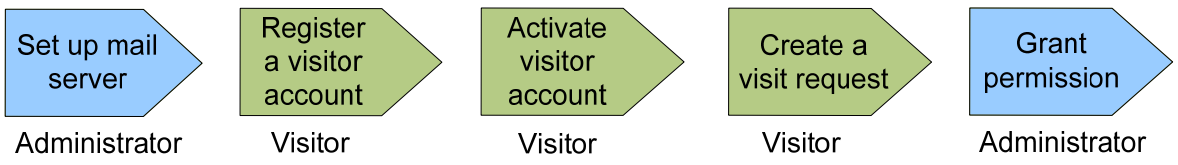


Figure 11-11

11.6 Visitor Self Registration

Visitors can create a visitor account over the Internet and request permission to access the premise.

The administrator needs to first set up the mail server on GV-VMWeb. The visitor will be able to register a visitor account, activate the account and create a visit request. The visit request will show up in GV-VMWeb for the administrator to grant or deny access.



11.6.1 Setting Up Mail Server in GV-VMWeb

The administrator must first set up the mail server in GV-VMWeb. The mail server will be used to send a confirmation e-mail to the visitor when they register an account.

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected.
2. Click **https://** and then **VMWeb** for SSL encrypted connection, or **VMWeb** for regular connection.
3. Enter a valid username and password for login. The GV-VMWeb page appears.
4. In the top-right corner, click **System Settings** and select **Visitor Web**.

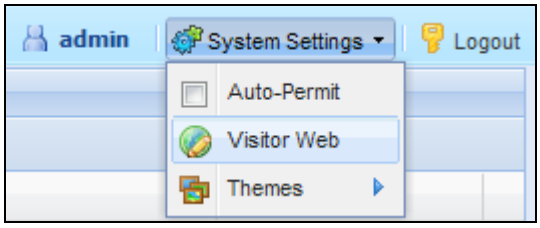


Figure 11-12

5. Under the Servers tab, set up the mail server.

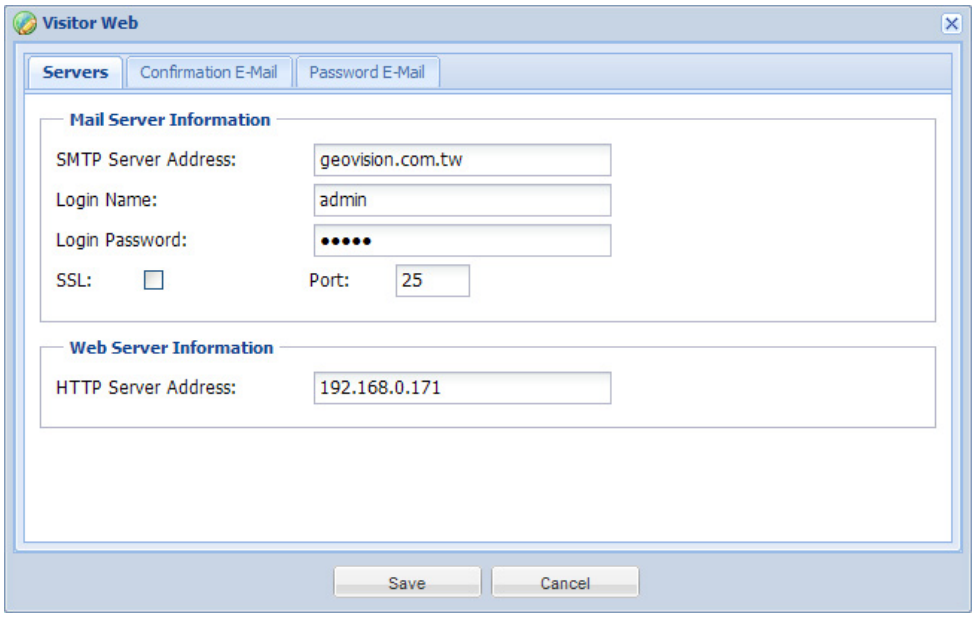


Figure 11-13

- **SMTP Server Address:** Type your mail server's URL address or IP address.
- **Login Name / Password:** Type the login name and password of the mail server.
- **SSL:** Select SSL if your e-mail server requires the SSL authentication for connection.

- **Port:** Keep the default port 25 or type a new port number for webmail providers that may use different SMTP port such as Yahoo and Hotmail.
- **HTTP Server Address:** Type the IP address or the domain name of the GV-ASManager.

6. Click the **Confirmation E-Mail** tab and type the **Sender Name**, **Sender Address**, **Mail Subject** and **Mail Message**. After registering a visitor account, a confirmation e-mail will be sent to the visitor and the visitor must click the activation link to confirm the account.

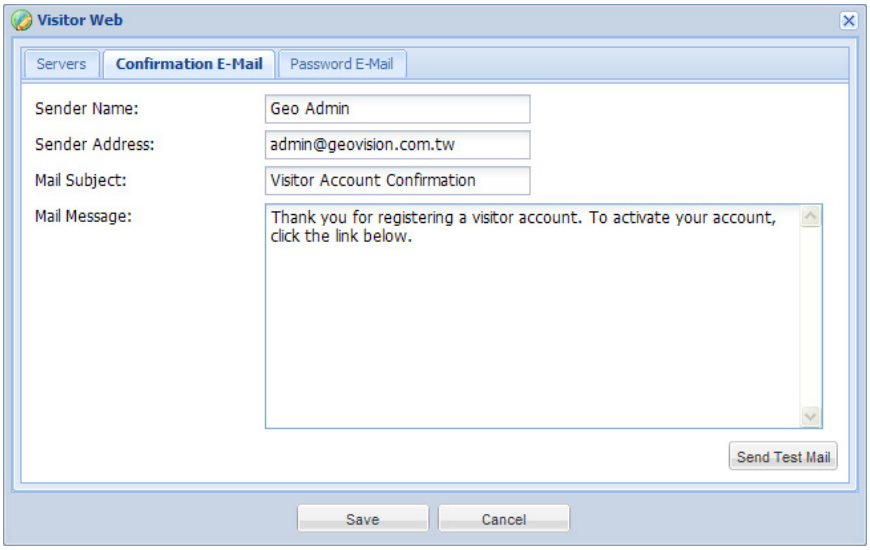


Figure 11-14

7. Click the **Password E-Mail** tab and fill out the information. The visitor will be able to retrieve a forgotten password by clicking the “Forgot your password?” link at the login page. An e-mail with the password will be sent to the visitor.

11.6.2 Creating a Visitor Account

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected. This web page appears.

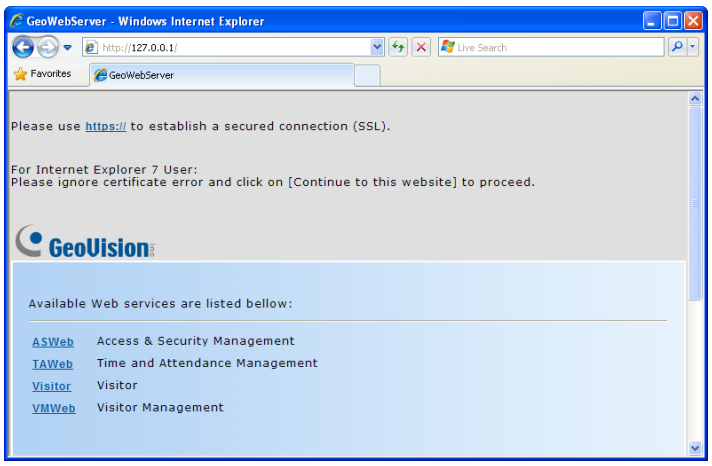

GeoWebServer - Windows Internet Explorer
http://127.0.0.1/
Favorites
GeoWebServer
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb Access & Security Management
TAWeb Time and Attendance Management
Visitor Visitor
VMWeb Visitor Management

Figure 11-15

2. Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** directly for regular connection. The Visitor Login page appears.

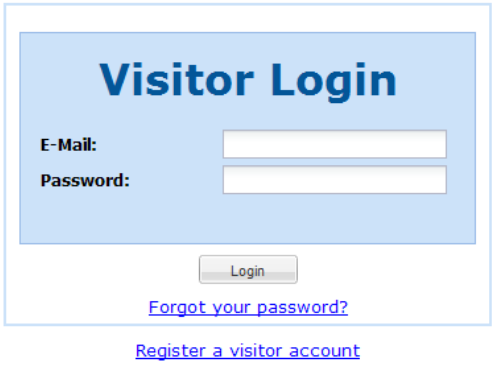


Figure 11-16

3. Click **Register a Visitor Account**. This window appears.

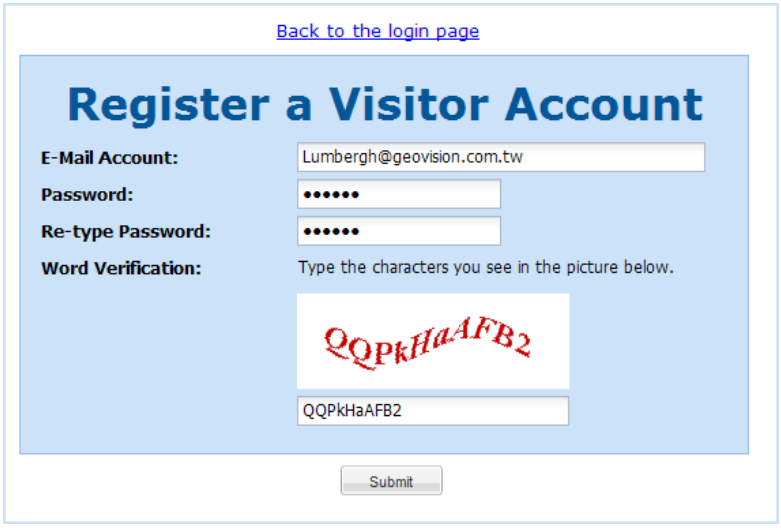


Figure 11-17

4. Type the e-mail address and type a password for the visitor account.
5. Type the characters for word verification.
6. Click **Submit**. A confirmation e-mail will be sent to the e-mail address shortly. Click the activation link in the e-mail to activate the visitor account.

11.6.3 Creating a Visit Request

After the visitor account is activated, the visitor can now log into his or her account to create a visit request.

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected. A web page appears.
2. Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** directly for regular connection. The Visitor Login page appears.
3. Type the visitor account and password, and click **Login**. This window appears.

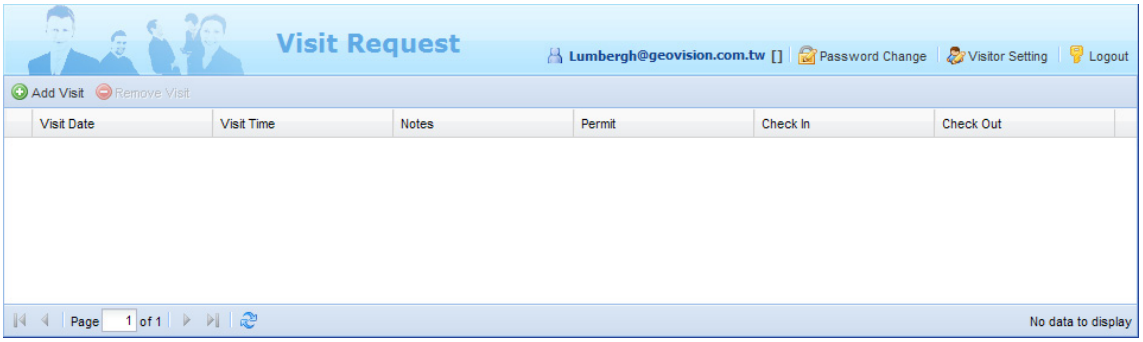


Figure 11-18

4. Click the **Visitor Setting** button to complete the visitor profile. Refer to *Creating Visitor Profile* earlier this chapter for more details.

5. Click the **Add Visit** button. This dialog box appears.

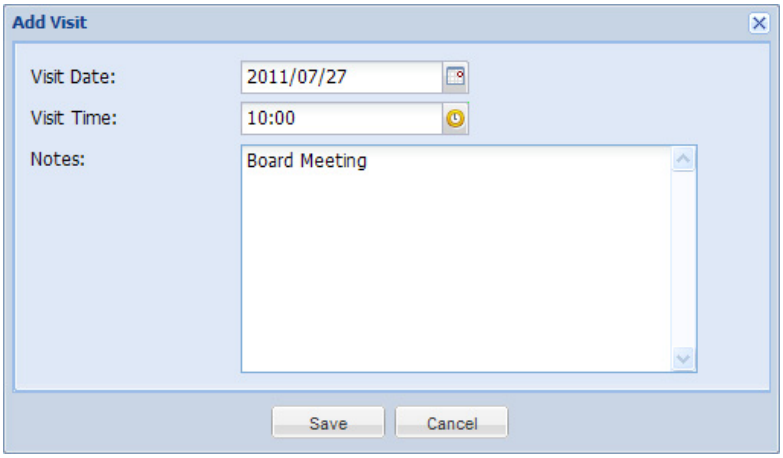


Figure 11-19

6. Specify the planned visit date and time.

7. Click **Save**.

When the administrator logs into GV-VMWeb, he or she can click the visitor's name to see the visit request submitted.

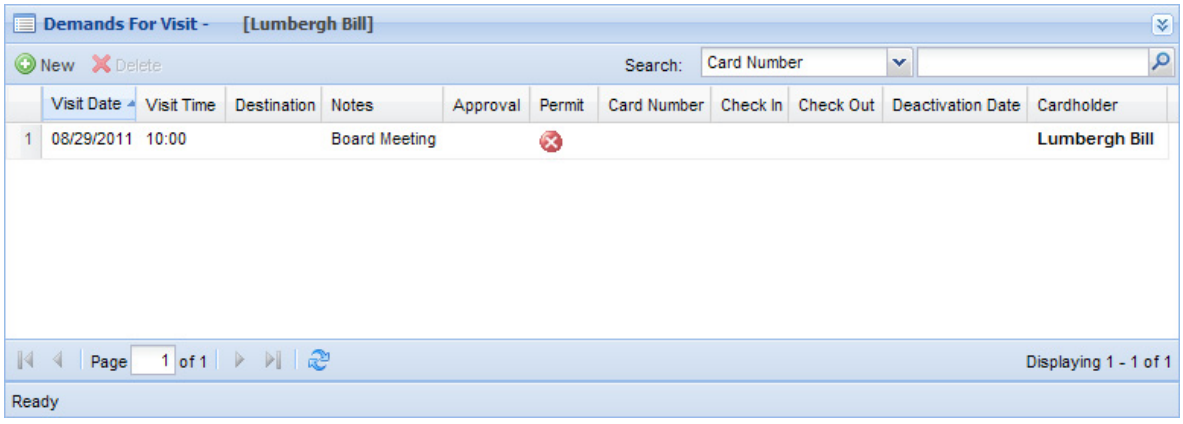


Figure 11-20

The administrator can double-click the visit request to grant access and assign visitor card to the visitor.

Chapter 12 Database Settings

Before you can run GV-ASManager, it is required to create a database or to upgrade your old database to fit the latest version of GV-ASManager. You can select either a **Microsoft Office Access** or **Microsoft SQL Server** to be the database of GV-ASManager.

If a database already exits, the GV-ASManager provides you the **Source Database** function to convert various database formats to be the GV-ASManager's (Access or SQL Server).

12.1 Starting the Database Tools

To start the Database Tools, you may use one of the methods:

1. If you log in the GV-ASManager for the first time, this message will pop up: "*Cannot open database. Would you like to set up database?".* Click **Yes**. The following Database Tools dialog box will appear.
2. If you have run the GV-ASManager, run **ASDBManager.exe** from the program folder to access the Database Tools.

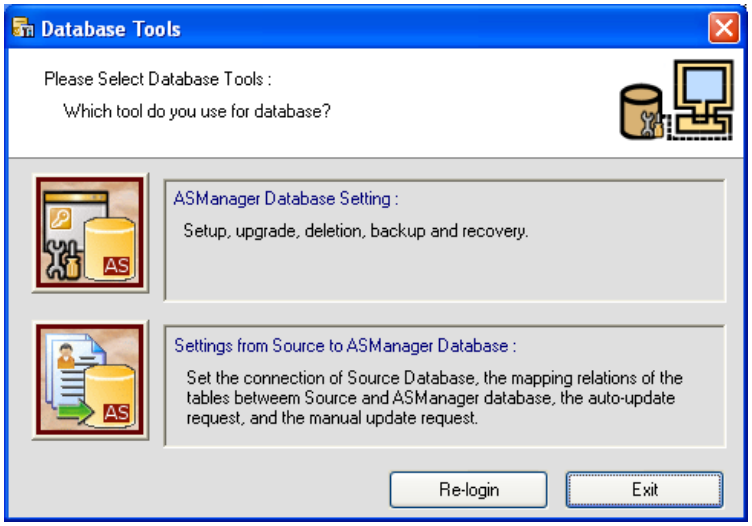

Database Tools
Please Select Database Tools :
Which tool do you use for database?
ASManager Database Setting :
Setup, upgrade, deletion, backup and recovery.
Settings from Source to ASManager Database :
Set the connection of Source Database, the mapping relations of the tables betweem Source and ASManager database, the auto-update request, and the manual update request.
Re-login
Exit

Figure 12-1

12.2 Creating a Database

You can select either Microsoft Office Access or Microsoft SQL Server as the database of GV-ASManager.

1. Click the **ASManager Database Setting** button on the Database Tools dialog box (Figure 12-1).
2. Click the **Setup MDB/MSSQL Database for ASManager** button. This dialog box appears.

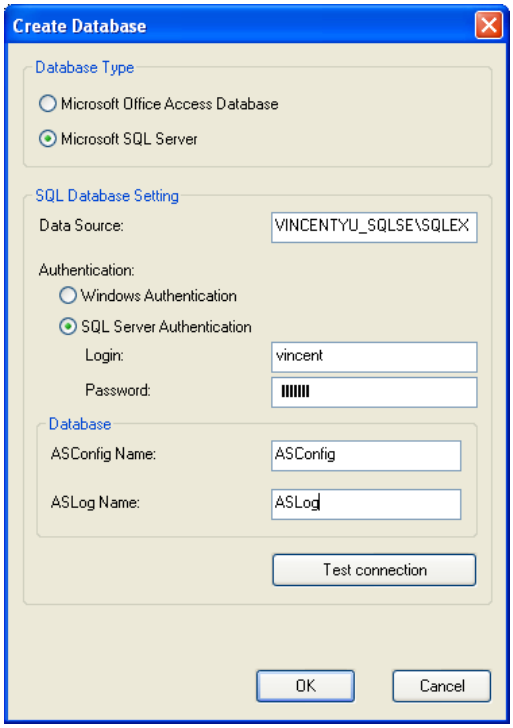


Figure 12-2

3. To use Access as the database, select **Microsoft Office Access Database** and click **OK**. The database is created in the local computer.
4. To use SQL Server as the database, select **Microsoft SQL Server.**
   a. Under the SQL Database Setting, type IP address or domain name of the SQL server in the Data Source field, and select its authentication way.
   b. Under the Database, name the databases for Configuration files and Log files that will be created on the SQL server separately.
   c. Click **Test Connection** to test the connection to the SQL server.
   d. Click **OK**. The databases are created in the SQL server.

12.3 Other Database Settings

You can upgrade, delete, back up and remove the database of GV-ASManager. Click **ASManager Database Setting** button on the Database Tools dialog box (Figure 12-1) to display the following dialog box and have further settings.

Figure 12-3

[Upgrade to latest database version] If an old database exits on the local computer, select this option to upgrade the version of the old database to the latest.

[Delete ASManager Database] Removes the database from the local computer or the SQL Server.

[Backup Database] Backs up the **Configuration** file.

[Recovery Database] Restores the backup **Configuration** file to the current computer or import it to another computer.

Note: To automatically back up Log and Image files, use the **Auto Backup** function. See *7.3 Startup and Backup Setup*.

12.4 Source Database Connection

The Source Database function can convert the databases of **OLE DB** and **Active Directory** to be the GV-ASManager's (Access or SQL Server). Click the **Setting from Source to ASManager Database** button on the Database Tools dialog box (Figure 12-1) to display the following dialog box and have further settings.

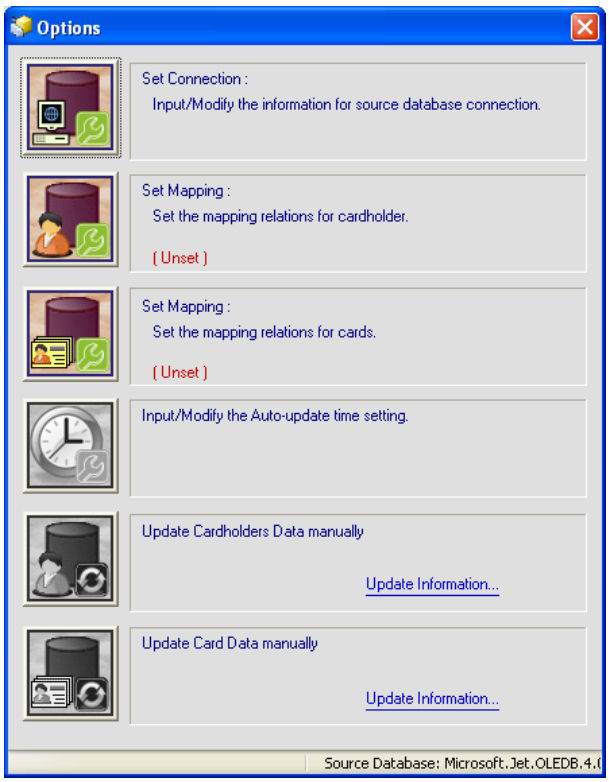


Figure 12-4

[Set Connection] Configures the connection to an active directory or an OLEDB provider.

[Set Mapping….for cardholder] Maps the cardholder fields between the GV-ASManager database and the source database.

[Set Mapping….for card] Map the card fields between the GV-ASManager database and the source database.

[Input/Modify the auto-update time setting] Specify a time to update the database automatically.

[Update Cardholders Data manually] Update the cardholder data manually.

[Update Card Data manually] Update the card data manually.

12.4.1 Converting Data from the Active Directory Database

1. Click the **Set Connection** button on the Options dialog box (Figure 12-4). The Source Database dialog box appears.
2. Select **Active Directory**. This dialog box appears.

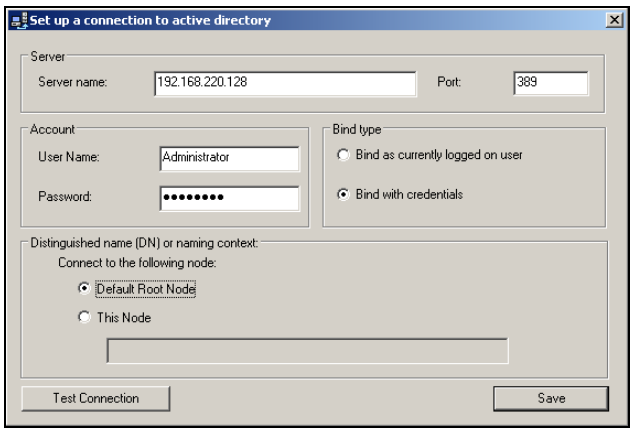


Figure 12-5

3. If you log in the local computer with the authorized username and password from the source database server, select **Bind as currently logged on user** and type the IP address or domain name of the server. If not, select **Bind with credentials**, type the IP address or domain name of the server and its login username and password.
4. Ensure the **Port** number matches that of the source database server.
5. Select **Default Root Node** to connect to the root node of the source database. Otherwise, select **This Node** and specify the node path.
6. Click **Test Connection** to connect to the source database server.
7. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 12-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
8. Click the **Update Card Data manually** button in the Options dialog box (Figure 12-4) to convert the card data from the source database to the GV-ASManager database immediately.
9. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 12-4) and specify the time in minutes.

12.4.2 Converting Data from the OLE Database

To convert data from the OLE database, you need to go through these instructions:

- **Connect an OLE database**
- **Map the cardholder data**
- **Map the card data**
- **Convert the data from the source database**

To connect an OLE database:

1. Click the **Set Connection** button on the Options dialog box (Figure 12-4). The Source Database dialog box appears.
2. Select **Other Database**. This dialog box appears.

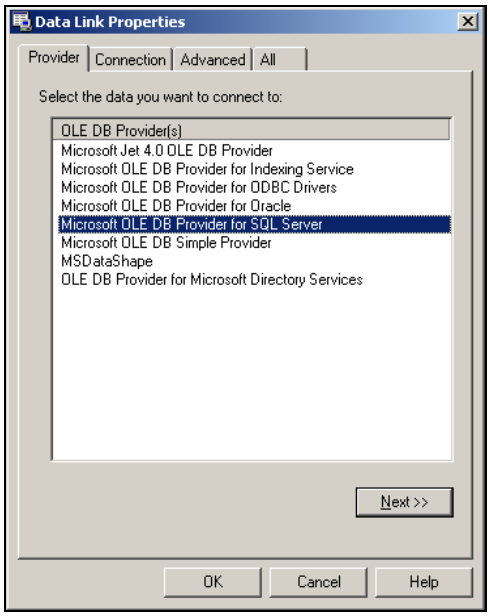


Figure 12-6

3. Select the OLE DB provider that you wish to connect to, and click **OK**. The connection dialog box appears. The dialog box varies depending on the OLE DB provider you choose. Here we select **Microsoft OLE DB Provider for SQL Server** as example.

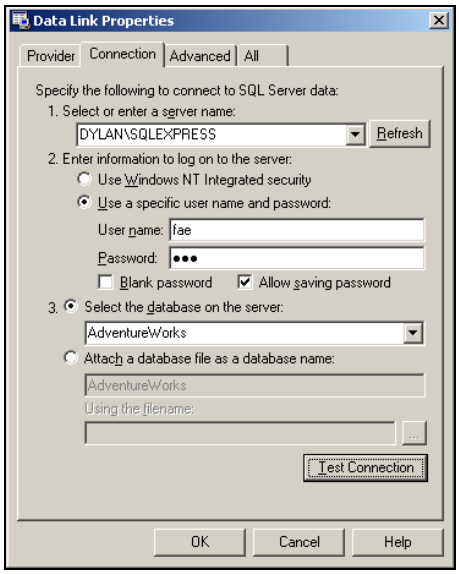


Figure 12-7

4. Type the IP address or domain name of the source database server, select its login authentication method, and select a specific database on the server. Click **Test Connection** to connect to the source database server.

To map the cardholder data:

1. Click the **Set the mapping relations for cardholders** button in the Options dialog box (Figure 12-4). This window appears.

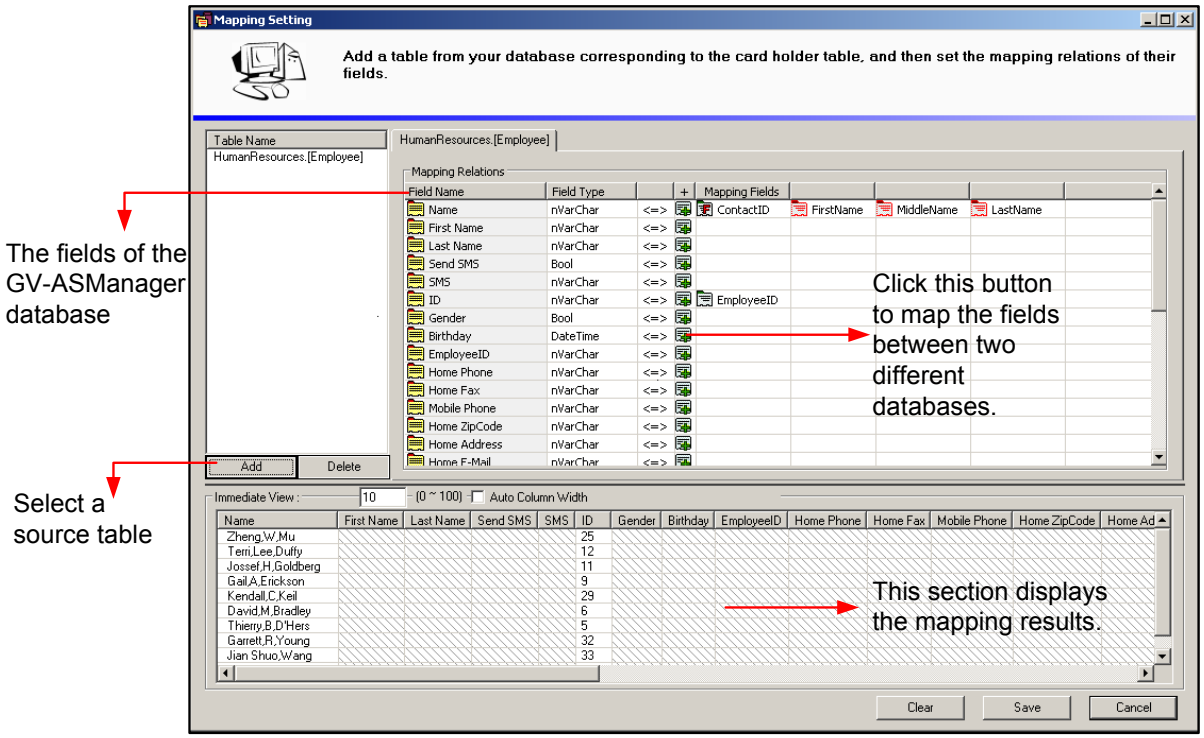


Figure 12-8

2. Click the **Add** button to select a related table on the source database.
3. Click the buttons to map each field of GV-ASManager database to a corresponding field of the source database.
4. In the following steps, we demonstrate how to map the **Name** filed as example. lick the button in the Name field. This dialog box appears.

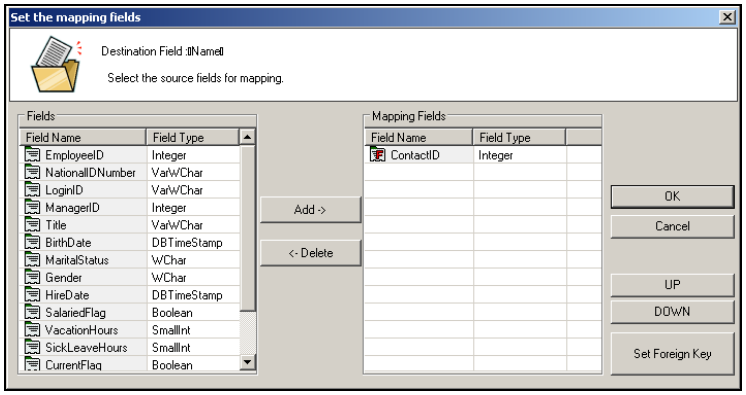


Figure 12-9

5. In the left side of the mapping field dialog box, select the field(s) of the source database corresponding to the Name field of the GV-ASManager database. Then click **Add**. In this example (Figure 12-9), the **Contact ID** field of the source database corresponds to the **Name** filed of the GV-ASManager database.

6. If the field of the source database, without having the data entered, is linked to an index or another table, click the **Set Foreign Key** button. This dialog box appears.

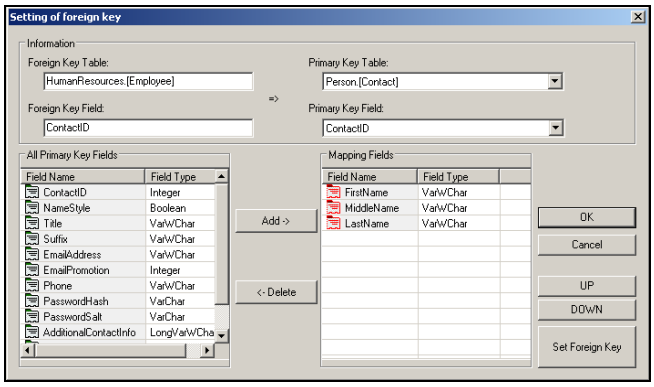


Figure 12-10

7. When the foreign key dialog box is open, the linked **Primary Key Table** and **Primary Key Field** should be displayed if the connection of the Foreign Key Table and Primary Key Table has been created. Otherwise, use the drop-down lists to select the Primary Key Table and Field.

8. In the left side of the foreign key dialog box, select the field(s) of the Primary Key Table corresponding to the field of the Foreign Key Table. In this example (Figure 12-10), the **Contact ID** field of “Human Resource (Employee)” Foreign Key Table is linked to the **First Name**, **Middle Name** and **Last Name** fields of “Person (Contact)” Primary Key Table.

9. Click **OK**. In the Mapping Setting window, you can see the mapping results. In the example (Figure 12-8), the **Name** field of the GV-ASManager database is mapped to the **Contact ID** field of the source database which includes **First Name**, **Middle Name** and **Last Name** (which are linked from the Primary Key Table).

To map the card data:

1. Click the **Set the mapping relations for cards** button in the Options dialog box (Figure 12-4). This window appears.

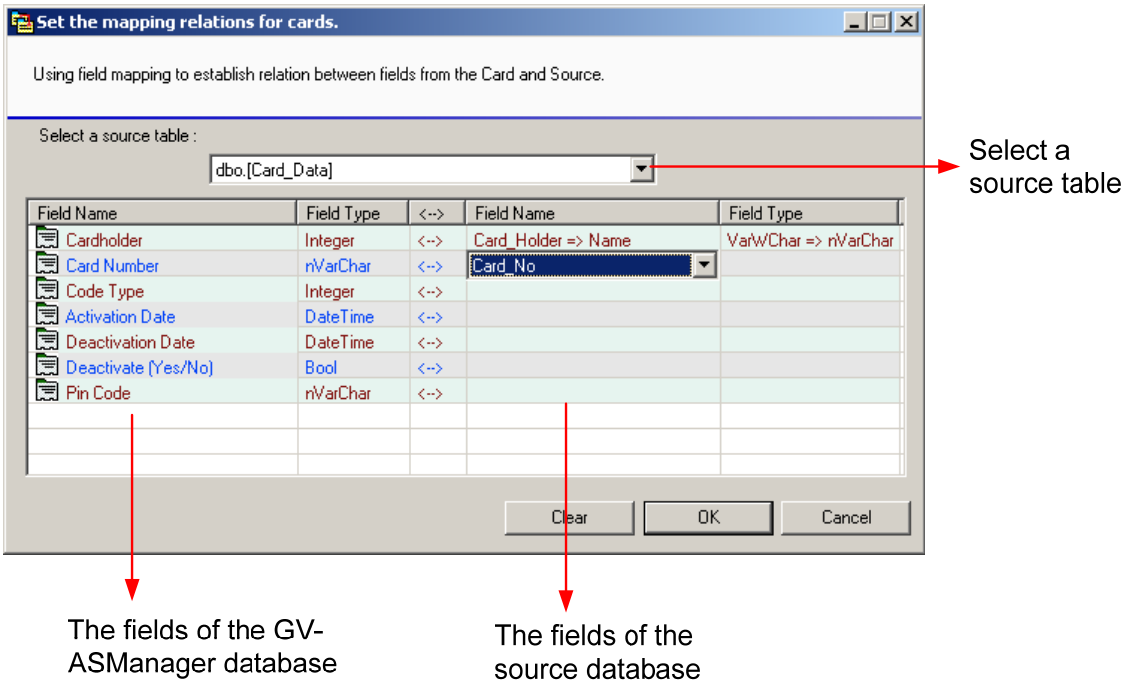


Figure 12-11

2. Select a related table on the source database.
3. Click the **Field Name** column on the right side to map each field of the GV-ASManager database and the source database.

To convert the data from the source database:

1. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 12-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
2. Click the **Update Card Data manually** button in the Options dialog box (Figure 12-4) to convert the card data from the source database to the GV-ASManager database immediately.
3. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 12-4) and specify the update time.

Chapter 13 Net Module Utility

With the **Net Module Utility** included in Software CD, you can change settings and update the firmware of the GV-AS Controller.

1. Insert Software CD, select **Install GeoVision V3.0.0.0 Access Control System**, click **Net Module Utility** and follow the onscreen instructions to install the program.
2. Run **Net Module Utility**. This window appears.

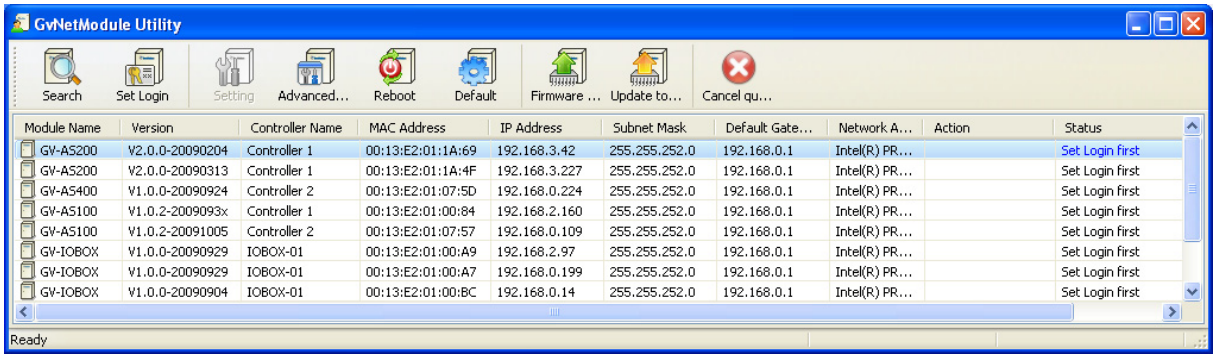

GvNetModule Utility
Search
Set Login
Setting
Advanced...
Reboot
Default
Firmware ...
Update to...
Cancel qu...
Module Name | Version | Controller Name | MAC Address | IP Address | Subnet Mask | Default Gate... | Network A... | Action | Status
GV-AS200 | V2.0.0-20090204 | Controller 1 | 00:13:E2:01:1A:69 | 192.168.3.42 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-AS200 | V2.0.0-20090313 | Controller 1 | 00:13:E2:01:1A:4F | 192.168.3.227 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-AS400 | V1.0.0-20090924 | Controller 2 | 00:13:E2:01:07:5D | 192.168.0.224 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-AS100 | V1.0.2-2009093x | Controller 1 | 00:13:E2:01:00:84 | 192.168.2.160 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-AS100 | V1.0.2-20091005 | Controller 2 | 00:13:E2:01:07:57 | 192.168.0.109 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-IOBOX | V1.0.0-20090929 | IOBOX-01 | 00:13:E2:01:00:A9 | 192.168.2.97 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-IOBOX | V1.0.0-20090929 | IOBOX-01 | 00:13:E2:01:00:A7 | 192.168.0.199 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
GV-IOBOX | V1.0.0-20090904 | IOBOX-01 | 00:13:E2:01:00:BC | 192.168.0.14 | 255.255.252.0 | 192.168.0.1 | Intel(R) PR... | Set Login first
Ready

Figure 13-1

The buttons on the window:

- **Search:** Click this button to locate any GV-AS Controller or GV-I/O device on the same LAN.
- **Set Login:** You can select the desired modules from the list, and click this button to log on to these modules with the same ID and password together.
- **Setting:** Click this button to change the Machine Name, IP address, 3DES Code, Device Port, login ID and password.
- **Advanced Setting:** Click this button to directly link to the Web interface of the selected module.
- **Reboot:** Click this button to perform a warm boot of the selected module. This operation will keep the current configuration.
- **Default:** Click this button to resets all configuration parameters to their factory settings. This may take 5 seconds to complete.
- **Firmware Update:** Click this button and assign the firmware file for update.
- **Update to the latest firmware version:** The GV-ASManager software comes with the latest GV-AS Controller firmware. Clicking this button can upgrade your GV-AS Controller firmware.

Chapter 14 Troubleshooting

Q1: GV-ASManager cannot connect to GV-AS Controller over the Internet.

There are several causes for this problem such as IP address conflict, incorrect connection settings and network failure. The following solution is to assign the fixed IP to the GV-ASManager and GV-AS Controller respectively. This way can determine if the problem is caused by the faulty devices and incorrect network settings.

1. Disconnect the hub or switch, which connects the GV-ASManager and GV-AS Controller, from the network.
2. Give the GV-ASManager a fixed IP address that is NOT used by another device, e.g. 192.168.0.154.

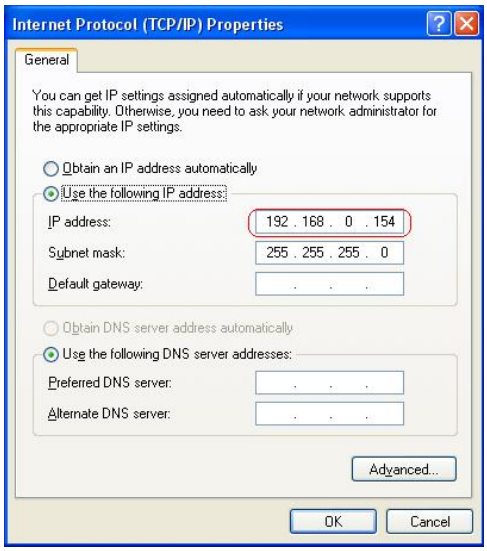

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 154
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 14-1

3. Reset the GV-AS Controller module and Ethernet module to factory defaults.
   a. Plug the GV-ASKeypad to the GV-AS Controller.
   b. Remove the jumper cap from the 2-pin **Default** jumper.
   c. Press the **Reset** button.
   d. Replace the jumper cap back to the 2-pin **Default** jumper.
   e. To reset the Ethernet Module, press and hold the **Default EN** button for 6 seconds.

4. Open the browser and enter the GV-AS Controller default address: http://192.168.0.100

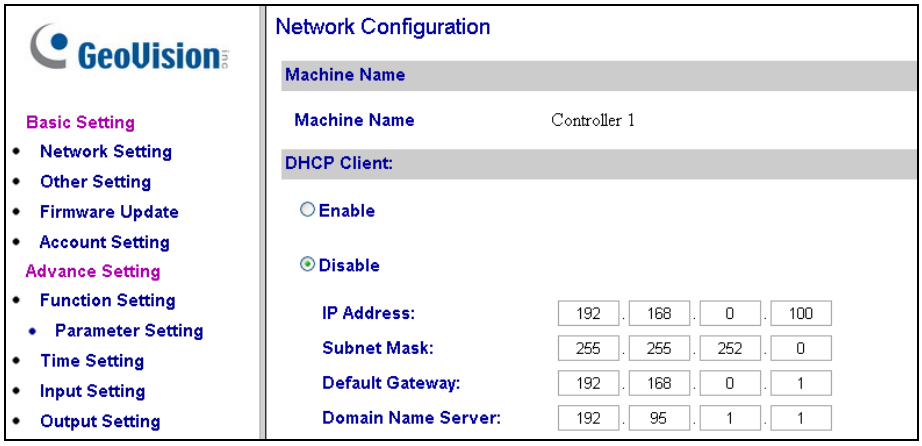


Figure 14-2

5. In the IP address field, give the GV-AS Controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.

6. On the GV-ASManager, enter the following settings:

   Controller ID: 1

   Network: TCP/IP

   IP: 192.168.0.XXX

   Port: 4000

   User: admin

   Password: admin

   Crypto key: 12345678

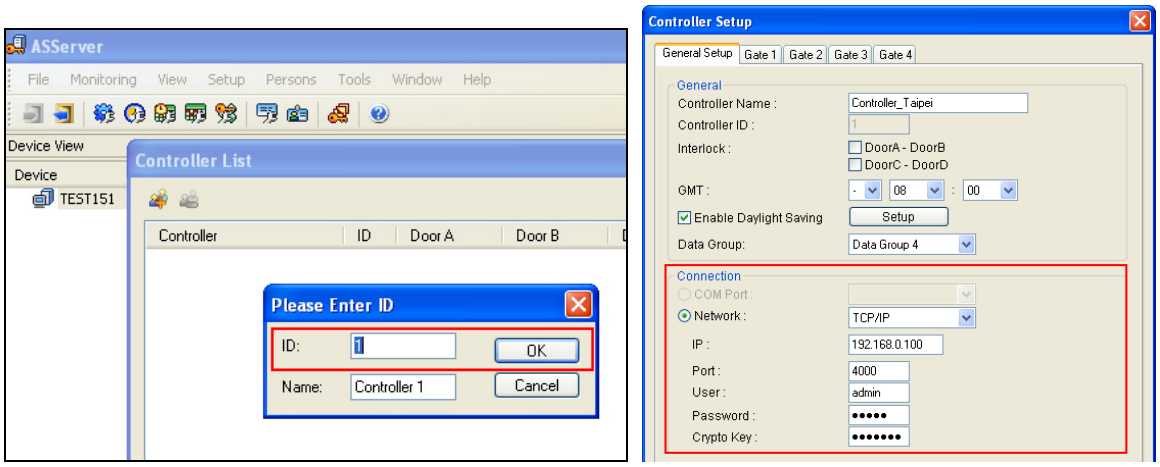


Figure 14-3

7. The connection between the GV-ASManager and GV-AS Controller should be established, and the connection icon should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

Q2: The connection established between the GV-ASManager and GV-AS Controller is interrupted.

This may be due to IP address conflict. Follow these steps to troubleshoot the problem:

1. Disconnect the hub or switch, which connects to the GV-ASManager and GV-AS Controller, from the network.
2. Run Windows **Command Prompt**. Take Classic Windows Start Menu for example, click **Start**, select **Accessories** and click **Command Prompt**.
3. Type **arp –d** and press **Enter**.

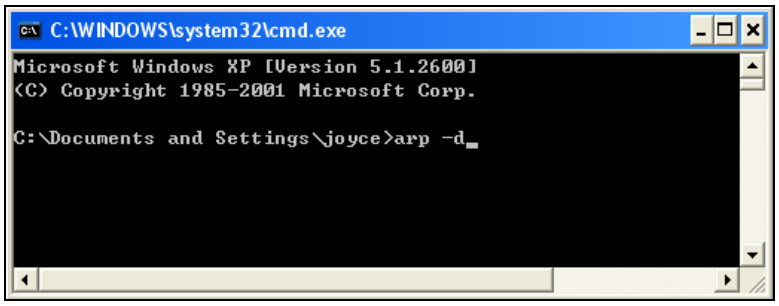


Figure 14-4

4. Give the GV-ASManager a fixed IP address that is NOT used by another device. See Figure 14-1.
5. Open the browser and enter the assigned IP address of GV-AS Controller. The Network Configuration page appears. See Figure 14-2.
6. In the IP address field, give the GV-AS Controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
7. On the GV-ASManager, enter the following settings. See Figure 14-3.

   Controller ID: 1

   Network: TCP/IP

   IP: 192.168.0.XXX

   Port: 4000

   User: admin

Password: admin

Crypto key: 12345678

8. The connection between the GV-ASManager and GV-AS Controller should be established, and the connection icon should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

Q3: GV-ASManager cannot receive card messages but the reader accepts the card when the connection between the GV-ASManager and GV-AS Controller is well established.

It may be due to memory failure in the GV-AS Controller. Reset both the GV-AS Controller module and the Ethernet module to factory settings. Refer to Step 3 in Question 1.

Q4: The GV-ASManager cannot retrieve the video from the DVR for playback.

1. Make sure the **Remote ViewLog Service** on **Control Center Server** is enabled on the DVR.
2. Make sure the time on the GV-ASManager and the DVR is consistent.
3. Make sure the event file you want to play back has been created completely on the DVR. For example, the assigned time length of every recorded event on the DVR is 5 minutes. The desired event of 5 minutes must have been displayed on the ViewLog Event List, so you can access the event file for playback.

Q5: After I add a card by presenting to the reader, the message "*Access Denied Invalid Card*" still appears

(For details on adding a card, see Step 1 in *4.3.1 Adding a Single Card.)*

It may be the card format is not compatible with the GV-AS Controller. For GV-AS100, GV-AS110, GV-AS120 and GV-AS400, ensure the format is 26~64 bits. Otherwise, send us the related information of your card format so that we can customize the format for you.

Q6: The GV-ASManager cannot receive card messages from the GV-Reader connected to the GV-AS Controller through RS-485 interface.

1. Make sure the GV-Reader is correctly wiring to the GV-AS Controller and Switch 4 on the GV-Reader is set to OFF.
2. Make sure the correct GV-Reader ID is set on the GV-AS Controller.

Q7: How can I find more help?

Visit our website at http:///www.geovision.com.tw

Write to us at support@geovision.com.tw

Appendix

A. Compatible IP Devices

This list provides the supported IP device brands. For detailed information on the supported IP devices, refer to Supported IP Camera List on GeoVision's Website:
http://www.geovision.com.tw/english/4_21.asp

GeoVision
ACTi
Arecont Vision
AXIS
Bosch
Canon
CNB
D-Link
Etrovision
Hikvision
IQinVision
JVC
MOBOTIX
Panasonic
Pelco
Sanyo
SONY
UDP
Verint
VIVOTEK

B. Event Notifications

- **"Alarm" events**

Type	Description
Force Open	Door <name> is forcibly open.
Duress	Duress function is triggered. See "Duress" in *1.2 Concepts*.
Tamper	Tamper Inputs are triggered. For hardware settings, see *Connecting Input Devices* in GV-AS Controller Hardware Installation Guide. For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*.
Fire Alarm	Fire Inputs are triggered. For hardware settings, see *Connecting Input Devices* in GV-AS Controller Installation Guide. For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*.
Held Open	Door <name> is held open over the specified time. See Step 2 and 5 in *4.2.2 Step 2: Configuration a Door.*
Access Denied	The access is rejected.

- **"Access" events**

Type	Description
Access Granted	The access from Cardholder <name> and Card <Number> is granted.
Access Denied: Invalid Card	The access is rejected because an unknown card is presented.
Access Denied: Card suspended	The access is rejected because Card <Number> is suspended.
Access Denied: Wrong PIN	The access is rejected because the PIN number entered is wrong.
Access Denied: Card Expired	The access is rejected because Card <Number> is expired.
Access Denied: Invalid schedule	The access is rejected because the user access is not on the programmed schedule.
Access Denied: Wrong Door	The access is rejected because the user has access to the wrong door.

Access Denied: APB (Duplicate Entries)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as successive entries, without exit, to a secure area.
Access Denied: APB (No Entry)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as exit, without entry, to a secure area.
Access Denied: APB (No Exit)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as entry, without exit, to a secure area.
Access Denied: Unknown Card	The access is rejected because the card format is not compatible.
Access Denied: Invalid Start Date	The access is rejected because Card <Number> is not enabled.
Access Denied: Previous Door Still Open (Interlock)	The access is rejected because the Interlock function is violated. The entry door is left unlocked. See “Interlock” at Step 5 in *4.2.1 Step 1: Configuring a Controller*.

- **“Event” events**

Type	Description
Force Open	Door <name> is forcibly open.
Duress	Duress function is triggered. See “Duress” in *1.2 Concepts*.
Tamper	Tamper Inputs are triggered. For hardware settings, see *Connecting Input Devices* in GV-AS Controller Installation Guide. For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*.
Fire Alarm	Fire Inputs are triggered. For hardware settings, see *Connecting Input Devices* in GV-AS Controller Installation Guide. For software settings, see Step 5 in *4.2.2 Step 2: Configuration a Door*.
Held Open	Door <name> is held open over the specified time. See Step 2 and 5 in *4.2.2 Step 2: Configuration a Door.*
Access Denied	The access is rejected.
Alarm Restored	Alarm sounds are cleared.
Forced Open-Restored	Force Open alarm is cleared.

Duress Restored	Duress alarm is cleared.
Tamper Restored	Tamper alarm is cleared.
Fire Alarm Restored	Fire alarm is cleared.
Held Open Restored	Held Open alarm is cleared.
Restored Alarm Failed	Fail to clear alarm sounds.
Clear Forced Open Event Failed	Fail to clear Force Open alarm.
Clear Duress Event Failed	Fail to clear Duress alarm.
Clear Tamper Event Failed-No Event Present	Fail to clear Tamper alarm.
Clear Fire Alarm Event Failed-No Event Present	Fail to clear Fire alarm.
Clear Held Open Event Failed	Fail to clear Held Open alarm.
Clear Access Denied Failed	Fail to clear Access Denied alarm.
Clear Tamper Event Failed-I/O Still Unclear	Fail to clear Tamper alarm because Tamper Inputs remain triggering.
Clear Fire Event Failed-I/O Still Unclear	Fail to clear Fire alarm because Fire Inputs remain triggering.
Door Open	Door <name> is open.
Door Close	Door <name> is close.
Door/Gate Unlock	Door <name> is unlocked.
Door/Gate Lock	Door <name> is locked.
Two Person Rule-Active	Two-person A/B rule is active when Card <number> is presented.
Two Person Rule-Confirm	Two-person A/B rule is confirmed when Card <name> is presented after the other AB card.
Two Person Rule-Inactive	Two-person A/B rule is violated when Card <name> is presented successively or the other AB Card isn't presented within 20 seconds.
Keypad Code Confirm	On the Card or Common mode, the password entered is correct.
Wrong Keypad Code	On the Card or Common mode, the password entered is wrong.

Release Mode	Door <name> is on the Release Mode. See Step 4 in *4.2.2 Step 2: Configuration a Door*.
Card or Common Mode	Door <name> is on the Card or Common Mode. See Step 4 in *4.2.2 Step 2: Configuration a Door*.
Card and PIN Code Mode	Door <name> is on the Card and PIN Code mode. See Step 4 in *4.2.2 Step 2: Configuration a Door*.
Card Mode	Door <name> is on the Card mode. See Step 4 in *4.2.2 Step 2: Configuration a Door*.
Fire Unlock Mode	Door <name> is unlocked after Fire Inputs are triggered. See “Fire Action” at Step 2 in *4.2.2 Step 2: Configuration a Door*.
Fire Lock Mode	Door <name> is locked after Fire Inputs are triggered. See “Fire Action” at Step 2 in *4.2.2 Step 2: Configuration a Door*.
Force Unlock Remotely	Door <name> is unlocked remotely from the control of GV-ASManager or GV-ASRemote server.
Force Lock Remotely	Door <name> is locked remotely from the control of GV-ASManager or GV-ASRemote server.
Disable Remote Door Lock Operation	The event of “Force Unlock Remotely” or “Force Lock Remotely” is cleared.
Force Unlock Locally	Door <name> is unlocked on the site of Door Controller.
Force Lock Locally	Door <name> is locked on the site of Door Controller.
Disable Local Door Lock Operation	The event of “Force Unlock Locally” or “Force Lock Locally” is cleared.
Reset	Door Controller <name> is reset.

C. E-Mail and SMS Alert Symbols

Icon	Description
	%M (Message): include related alert message.
	%T (Controller): include door controller's name.
	%D (Door): include triggered door's name.
	%L (Local Time): include local time.
	%U (UTC): include UTC time.
	%N (Card Number): include card number.
	%H (Card Holder Name): include cardholder name.
	%G (Gender): include cardholder's gender.
	%E (Employee ID): include employee ID.
	%Y (Company): include company name.
	%P (Department): include department name.
	%F (Office): include office name.
	%C (Photo): include cardholder photo.
	%S (Snapshot): include snapshot.

D. Controller Status

Status	Description
Disconnected (Login Failed)	The username, password or crypto key (3DES) entered is wrong.
Disconnected (Duplicate Connection)	Another GV-ASManager is connecting with the GV-AS Controller.
Disconnected (Hardware Error)	The Controller ID entered is wrong. Or GV-AS Controller errors occur.